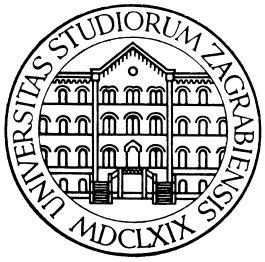
Sveučilište u Zagrebu
PMF–Matematički odsjek

Mladen Vuković

TEORIJA SKUPOVA

predavanja



Zagreb, siječanj, 2015.

Sadržaj

Predgovor

Ovaj materijal nastao je na osnovu zabilješki iz kolegija *Teorija skupova* koji više od deset godina predajem na Matematičkom odsjeku Prirodoslovno–matematičkoog fakulteta, Sveučilište u Zagrebu. Ovaj materijal je prije svega namijenjen studentima koji slušaju kolegij *Teorija skupova*, odnosno trebaju polagati ispit iz tog kolegija. No, nadam se da materijal može biti zanimljivim svakome koga zanimaju osnove matematike, odnosno njeno zasnivanje.

Želim naglasiti da ovo nije skripta. To znači da nije proveden postupak recenzije. Time nikako ne želim reći da imam opravdanje za greške (raznih vrsta) kojih sigurno ima. Svaki ispravak, ili pak sugestiju, koji bi mogli doprinijeti poboljšanju ovog teksta, rado ću prihvatiti.

Zahvaljujem se dr. sc. Vedranu Čačiću i prof. dr. sc. Juraju Šiftaru koji su pročitali čitav tekst, te svim studentima koji su me upozorili na greške.

U Zagrebu, studeni 2014. Mladen Vuković

Uvod

Sadržaj kolegija je pokriven ovim rukopisom. Štoviše, neki dijelovi rukopisa se ne predaju, a dodani su radi lakšeg razumijevanja teksta. To su prije svega zadaci i njihova rješenja. Rukopis, a i kolegij, podijeljeni su u dva glavna dijela: §1. *Naivna teorija skupova* i §2. *Aksiomatska teorija skupova*. Važno je na početku naglasiti da je glavni cilj prvog poglavlja motivirati uvođenje aksioma.

Sada navodimo knjige koje postoje u biblioteci PMF–MO u Zagrebu o teoriji skupova, a mogu pomoći za ovaj kolegij. Knjige nisu poredane po abecedi već po važnosti za kolegij.

1. W. Just, M. Weese, *Discovering Modern Set Theory 1*, American Mathematical Society, 1996.

2. K. Kunen, *Set Theory—An Introduction to Independence Proofs*, North–Holland, 1992.

3. P. Papić, *Teorija skupova*, HMD, Zagreb, 1999.

4. J. Shoenfield, *Axioms of Set Theory*, Handbook of Math. Logic, J. Barwise (ed.), North–Holland, 1985.

5. T. Jech, *Set Theory*, The Third Millenium Edition, Springer, 2000.

Svakako preporučamo knjižice iz biblioteke Moderna matematika od Školske knjige: N. J. Vilenkin, *Priče o skupovima*, J.–L. Krivine, *Aksiomatička teorija skupova*, te Z. Šikić, *Kako je stvarana novovjekovna matematika*.

Istaknimo glavne crtice u razvoju teorije skupova. Osnivač teorije skupova je Georg Cantor. Radove o teoriji skupova objavljivao je od 1871. do 1883. godine.

Georg Cantor, 1845.–1918.

Poseban zamah razvoju teorije dao je B. Russell otkrićem paradoksa. To je rezultiralo razvojem aksiomatske teorije skupova. Prvi prijedlog aksiomatizacije dao je E. Zermelo, 1908. godine. Zermelo je dokazao da se svaki skup može dobro urediti. Nakon velikih kritika njegovog neočekivanog rezultata, Zermelo je pobrojao aksiome koje je koristio. A. Fraenkel je 1922. godine precizirao shemu aksioma separacije. Zatim su A. Fraenkel i T. Skolem predložili shemu aksioma zamjene kao još jedan novi aksiom. J. von Neumann je eksplicirao aksiom dobre utemeljenosti i definirao ordinalne brojeve.

U ovom kratkom osvrtu na povijesni razvoj teorije skupova istaknut ćemo još samo da je 1938. godine K. Gödel dokazao relativnu konzistentnost Zermelo–Fraenkelove teorije skupova s aksiomom izbora i hipotezom kontinuuma, te je 1963. godine P. Cohen dokazao nezavisnost hipoteze kontinuuma sa Zermelo–Fraenkelovom teorijom skupova.

0.1 Osnovne napomene na početku

Osnovno pitanje ovog kolegija je:

Što je skup?

U **naivnoj teoriji** skupova odgovor je "jednostavan":

Skup je primitivan pojam, i kao takav se ne definira.
Smatramo da već imate izgrađenu intuiciju o pojmu skupa.
Skup je kolekcija objekata koji zajedno čine cjelinu.

Na takvom nedefiniranom i vrlo nejasnom pojmu skupa Cantor je izgradio veliki dio teorije skupova. Poteškoće koje su se pri tome javile (paradoksi i nerješivi problemi – o tome ćemo kasnije) pokušale su se izbjeći na razne načine (teorija tipova; teorija klasa, ...). No, teško je prevladati teškoće ako već na samom početku imamo klimave

temelje. Teorija skupova se mora graditi kao i svaka druga matematička teorija – zadavanjem aksioma.

U svojim istraživanjima tvorac teorije skupova Cantor nije se eksplicitno pozivao na neke aksiome o skupovima. Međutim, analizom njegovih radova može se zaključiti da se skoro svi teoremi koje je on dobio mogu izvesti iz sljedeća tri aksioma:

1. AKSIOM EKSTENZIONALNOSTI
   Dva skupa su jednaka ako imaju iste elemente.

2. PRINCIP KOMPREHENZIJE
   Za unaprijed dano svojstvo $\varphi(x)$ postoji skup čiji su elementi baš oni koji objekti imaju to svojstvo, tj. $\{x : \varphi(x)\}$ je skup.

3. AKSIOM IZBORA
   Za svaki neprazan skup postoji bar jedna funkcija čiji su argumenti neprazni podskupovi tog skupa, a slike su elementi argumenata.

Kada je teorija već postala priznata u matematičkom svijetu pojavili su se **paradoksi** – nešto što se nikad prije nije dogodilo. (Paradoks nije isto što i kontradikcija. Paradoks je tvrdnja čiji je dokaz logički neupitan, ali je intuitivno sama tvrdnja vrlo upitna.) Sada navodimo Russellov paradoks.

Russellov paradoks: $R = \{x \ : \ x \ \text{ je skup i } \ x \notin x\}$ nije skup.

Dokažimo da R nije skup. Pretpostavimo da je R skup. Tada možemo postaviti pitanje vrijedi li $R \in R$. Pretpostavimo prvo da vrijedi $R \in R$. To znači da je R element skupa R, pa ispunjava svojstvo koje ispunjavaju svi njegovi elementi, tj. $x \notin x$, odnosno za R to znači $R \notin R$. Time smo iz pretpostavke $R \in R$ dobili $R \notin R$, tj. dobili smo kontradikciju. Zaključujemo da mora vrijediti $R \notin R$. No, tada R ispunjava definicijski uvjet za skup R. To znači da je R jedan element skupa R, odnosno imamo $R \in R$. Opet smo dobili kontradikciju. Zaključujemo da pretpostavka da je R skup vodi na kontradikciju, tj. kolekcija R nije skup.

Bertrand Russell, 1872.–1970.

Što je to zapravo paradoksalno u *Russellovom paradoksu*? Russell je dao prvi primjer kolekcije objekata koja nije skup, te je na taj način ukazao da Cantorov princip komprehenizije ne moženo primjenjivati prilikom izgradnje skupova. To znači da nemamo nikakve kriterije kako graditi skupove. Treba spomenuti da postoje i drugi paradoksi naivne teorije skupova. Primjerice to su i *Cantorov paradoks skupa svih skupova*, te *Buralli–Fortijev paradoks*. Navest ćemo ih kasnije, kao i neke druge paradokse u naivnoj teoriji skupova. Možemo postaviti pitanje jesu li primjerice sljedeće kolekcije skupovi:

$\{x \ : \ \text{postoji bijekcija između skupa } x \ \text{ i skupa } \ \mathbb{N}\}$ (nije skup)

$\{x : \ x \ \text{ je diferencijabilna realna funkcija na skupu } \ \mathbb{R}\}$ (to je skup)

$\{x \ : \ x \ \text{ je skup takav da } \ \forall y \forall z(y \in z \in x \to y \in x)\}$ (nije skup)

$\{x \ : \ \text{postoji binarna operacija } \ \circ \ \text{ takva da je } \ (x, \circ) \ \text{ grupa}\}$ (nije skup)

Kasnije ćemo dati argumente zašto pojedina gornja kolekcija jeste, odnosno nije, skup.

Nadalje ćemo svaku kolekciju objekata nazivati **klasa**. Odnosno, ako je φ neko svojstvo tada ćemo kolekciju $\{x : \varphi(x)\}$ nazivati klasa. Neke klase su skupovi, a neke nisu. Klase koje nisu skupovi nazivaju se **prave klase**. Primjerice klasa iz Russellovog paradoksa je prava klasa. Intuitivno, klasa x je skup ako postoji klasa y takva da vrijedi $x \in y$.

Glavni zaključak nakon paradoksa je da u teorji skupova ne smijemo graditi skupove pomoću skupova koji nisu još izgrađeni – to se upravo događa primjenom principa komprehenzije. To znači da skupove moramo graditi po **nivoima**. Izgradnju skupova po nivoima omogućava aksiomatski pristup. Prije nego što napišemo aksiome Zermelo–Fraenkelove teorije skupova, koju ćemo kratko označavati sa `ZF`, pokušat ćemo opisati što želimo da aksiomi govore.

Ne zanimaju nas skupovi sljedećeg oblika (takvi primjeri su obično u školskim udžbenicima): skup svih samoglasnika u riječi ABRAKADABRA, skup svih djevojčica 5a razreda OŠ Retkovec u Zagrebu, skup svih filmova koji su prikazani u zagrebačkim kinima ove godine, ... A kakvi nas onda skupovi zanimaju? Želimo izgraditi teoriju koja bi na neki način bila temelj matematike. Primjerice to znači da bismo u njoj mogli definirati prirodne brojeve (a onda na standardni način i ostale skupove brojeva; to ćemo kasnije ilustrirati).

Prije strogih definicija moramo upozoriti na neke "loše" navike u vezi skupova. Obično se skupovi zamišljaju kako nekakve klase "atoma", tj. članova koji nemaju nikakvih dijelova. To znači da bi na početku izgradnje teorije skupova morali pretpostaviti egzistenciju nekakvih atoma ili praelemenata. No, može se pokazati da to nije nužno. Dovoljno je pretpostaviti da postoji skup koji nema niti jednog elementa, tj. prazan skup. Upravo je prazan skup jedini "atom" koji ćemo koristiti prilikom

izgradnje teorije skupova. Zatim, "loša" navika je da se teško prihvaća da skupovi mogu biti elementi drugih skupova. Jednostavan primjer takvog skupa je primjerice partitivni skup čiji su elementi svi podskupovi zadanog skupa. U teoriji skupova elementi svakog skupa su skupovi.

0.2 Kumulativna hijerarhija

Kada primjerice želimo napisati aksiome koji će opisivati prirodne brojeve mi imamo dobro izgrađen (ili nam se bar tako čini) intuitivan pojam prirodnog broja. Slična je situacija i s drugim pojmovima. Navedimo neke strukture i pripadne aksiomatizacije:

Teorija brojeva – Peanova aritmetika
Intuicija polja $\mathbb{R}$ *– aksiomi za* $\mathbb{R}$
Primjeri raznih grupa – aksiomi teorije grupa
Primjeri raznih vektorskih prostora – aksiomi vektorskog prostora

Prilikom aksiomatizacije teorije skupova imamo jedan veliki problem. Što intuitivno znači pojam skupa? Koju strukturu mi zapravo želimo opisati aksiomima? Danas se smatra da aksiomatski trebamo opisati strukturu sljedećih objekata:

$$\begin{aligned} V_0 &= \emptyset \\ V_1 &= \{\emptyset\} = \mathcal{P}(V_0) \\ V_2 &= \{\emptyset, \{\emptyset\}\} = \mathcal{P}(V_1) \\ &\vdots \end{aligned}$$

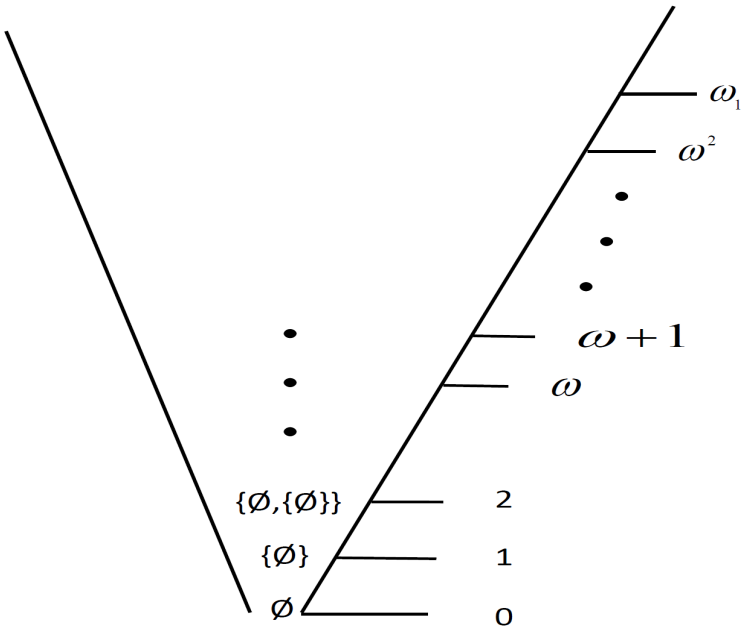
Odnosno, sasvim precizno to bismo rekurzivno definirali ovako:

$$\begin{aligned} V_{\alpha+1} &= \mathcal{P}(V_\alpha) \\ V_\beta &= \bigcup_{\alpha<\beta} V_\alpha \end{aligned}$$

gdje je α proizvoljan ordinalni broj (nivo!), a β je ordinalni broj koji nema neposrednog prethodnika. Tada klasu

$$V = \bigcup_{\alpha \in On} V_\alpha$$

nazivamo **kumulativna hijerahija**. Sa On je označena klasa svih ordinalnih brojeva. Kasnije ćemo objasniti, a i strogo definirati, što su to ordinalni brojevi. Na sljedećoj slici ilustriramo kumulativnu hijerarhiju.



Napomena 0.1. *Ovdje ćemo pokušati objasniti razliku između skupova i pravih klasa. Prije smo bili naveli princip komprehenzije:* ako je φ neko svojstvo tada ono definira skup $\{x : \varphi(x)\}$. *Vidjeli smo da to nija dobra ideja za izgradnju teorije skupova, jer dobivamo i paradokse. Mogli bi reći da neka svojstva imaju "preveliki" doseg tako da ne definiraju skupove. Za svako svojstvo φ (točnije: svaku formulu ZF teorije!) kolekciju objekata $\{x : \varphi(x)\}$ nazivamo klasa. Većina uobičajnih operacija koje se koriste u matematici ne vode do klasa koje su "prevelike", te to ne stvara nikakve probleme. Osnovne (intuitivne) zahtjeve o skupovima navest ćemo u sljedećih nekoliko točaka:*

(i) Svaka podklasa skupa je skup. Odnosno, za svaki skup A i svako svojstvo φ, postoji skup svih $x \in A$ za koje vrijedi $\varphi(x)$. Kasnije ćemo ovaj zahtjev formulirati kao shemu aksioma separacije *ZF teorije.*

(ii) Skupovi su zatvoreni na osnovne operacije kao što su unija, presjek i partitivni skup.

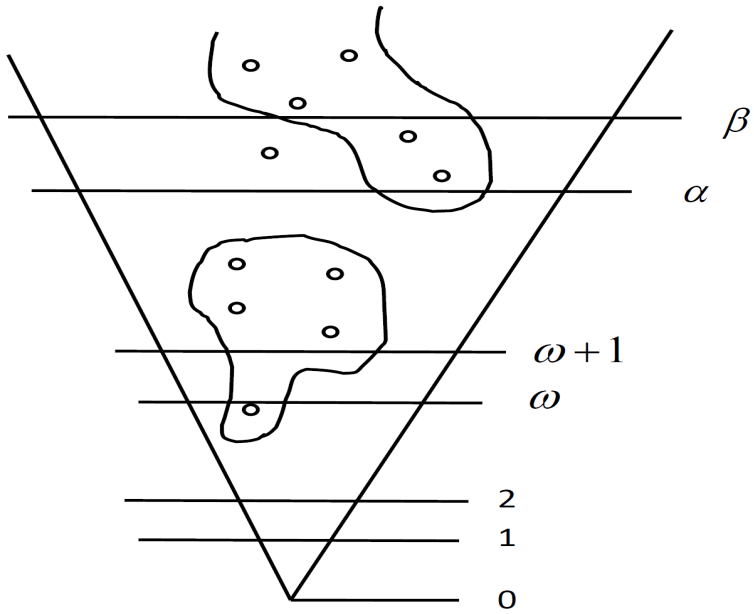
(iii) Skupovi su zatvoreni na slike funkcija. Odnosno, ako je f neka funkcija na skupovima i A je skup tada je $\{f(x) : x \in A\}$ također skup. Kasnije ćemo ovaj zahtjev formulirati kao shemu aksioma zamjene *ZF teorije.*

(iv) Ako je neka klasa X element neke druge klase Y tada je X skup. Ovo je najmanje intutivno jasan zahtjev. Povezan je s idejom kumulativne hijerarhije – svaki skup gradimo na nekom nivou.

Sada ćemo pokušati objasniti zašto navedene klase na strani 4 jesu, odnosno nisu skupovi. Klasa $\{x$: postoji bijekcija između skupa x i skupa $\mathbb{N}\}$ nije skup, jer na svakom nivou kumulativne hijerahije postoje prebrojivi skupovi, a onda ne postoji neki "završni" nivo na kojem je ta klasa izgrađena. Isti argument bi naveli prilikom objašnjenja da klase $\{x : x$ je skup takav da $\forall y \forall z(y \in z \in x \rightarrow y \in x)\}$ i $\{x$: postoji binarna operacija $\circ$ takva da je $(x, \circ)$ grupa$\}$ nisu skupovi. Klasa $\{x : x$ je diferencijabilna realna funkcija na skupu $\mathbb{R}\}$ je skup, jer se skup $\mathbb{R}$ konstruira na točno određenom nivou kumulativne hijerarhije.

Primijetimo još samo na kraju ove priče o klasama da paralelno s razlikom klasa i skupova postoji i razlika između funkcija i operacija koje su prevelike da bi mogle biti identificirane sa skupom uređenih parova. Primjerice $A \mapsto \mathcal{P}(A)$ je **skupovna operacija**, *ali nije funkcija.*

Na sljedećoj slici želimo posebno naglasiti da su skupovi ograničeni s nivoima, dok prave klase nisu.



0.3 Neki aksiomi Zermelo–Fraenkelove teorije

Aksiomi o skupovima bit će većinom sljedećeg oblika:

> *ako je A skup (ili više skupova) tada operacija F primjenjena na A opet daje (novi) skup.*

No, prije takvih aksioma iskazujemo dva osnovna aksioma `ZF` teorije skupova. Želimo još istaknuti da aksiome teorije `ZF` gradimo pomoću varijabli, zagrada, logičkih veznika: $\neg$, $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$, kvantifikatora: $\forall$ i $\exists$, te simbola $\in$ i $=$.

U daljnjim izlaganjima koristit ćemo i relacijske simbole $\subset$ i $\subseteq$. To nisu osnovni simboli jezika, već su pokrate za sljedeće iskaze:

$$x \subseteq y \;\Leftrightarrow\; \forall z(z \in x \rightarrow z \in y)$$

$$x \subset y \;\Leftrightarrow\; \forall z(z \in x \rightarrow z \in y) \;\wedge\; x \neq y$$

Prvo ističemo aksiom koji iskazuje kriterij za jednakost skupova.

Aksiom ekstenzionalnosti
Ako su x i y skupovi takvi da je $x \subseteq y$ i $y \subseteq x$ tada je $x = y$.
Odnosno, formalno:

$$\forall x \forall y \Big(\forall z(z \in x \leftrightarrow z \in y) \rightarrow x = y \Big)$$

Taj aksiom koristimo prilikom dokazivanja skupovnih identiteta. Iz aksioma ekstenzionalnosti posebno slijedi primjerice $\{1,2,3\} = \{3,1,2\}$ i $\{1,2,2,3,1\} = \{1,2,3\}$.

Sljedeći aksiom je aksiom egzistencije. Iz tog aksioma slijedi da postoji barem jedan skup.

Aksiom praznog skupa: postoji skup koji ne sadrži niti jedan element, tj.

$$\exists x \forall y(y \notin x)$$

Iz aksioma ekstenzionalnosti slijedi da je takav skup jedinstven. Iz tog razloga možemo uvesti oznaku za taj jedinstveni objekt: $\emptyset$.

Sada navodimo još neke aksiome teorije `ZF`, i to one koji su nam najpotrebniji i najrazumljiviji.

Aksiom partitivnog skupa: ako je x skup tada je klasa svih njegovih podskupova također skup, tj.

$$\forall x \exists y \forall z(z \in y \leftrightarrow z \subseteq x)$$

Iz aksioma ekstenzionalnosti slijedi jedinstvenost partitivnog skupa, pa uvodimo oznaku $\mathcal{P}(x)$.

Aksiom para: za svaka dva skupa x i y postoji skup čiji su x i y jedini elementi, tj.

$$\forall x \forall y \exists z \forall u \Big(u \in z \leftrightarrow (u = x \vee u = y) \Big).$$

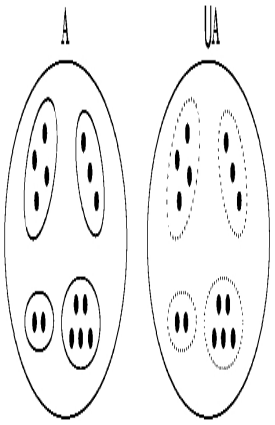
Iz aksioma ekstenzionalnosti slijedi jedinstvenost (neuređenog) para, pa uvodimo oznaku $\{x, y\}$.

Iz aksioma para slijedi da za svaki skup x postoji skup $\{x, x\}$. Po dogovoru taj skup označavamo sa $\{x\}$. Istaknimo koje skupove za sada znamo: $\emptyset$, $\{\emptyset\}$, $\{\emptyset, \{\emptyset\}\}$, ... No, iz do sada navedenih aksioma ne slijedi čak ni egzistencija trojke, tj. ako su x, y, z skupovi tada još ne možemo tvrditi da je $\{x, y, z\}$ skup. Posebno, ne možemo dokazati egzistencija nekog beskonačnog skupa. Primjenom aksioma unije slijedit će da za svaki $n \in \mathbb{N}$ postoji n–člani skup.

Aksiom unije: za svaki skup je klasa elemenata svih njegovih elemenata ponovno skup, tj.

$$\forall x \exists y \forall z (z \in y \leftrightarrow \exists t (t \in x \wedge z \in t)).$$

Pokušat ćemo objasniti aksiom unije na jednom primjeru. Neka je dan skup $A = \{\emptyset, \{b, c\}, \{d\}\}$. Tada aksiom unije tvrdi da je klasa objekata, koji su elementi nekog elementa od A, također skup. U ovom slučaju to znači da je $\{b, c, d\}$ također skup. Na sljedećoj slici ilustriramo aksiom unije.



Primjenom aksioma ekstenzionalnosti slijedi da je skup y, čija se egzistencija tvrdi u aksiomu unije, jedinstven. Za dani skup x sa $\cup x$ označavamo skup čija se egzistencija tvrdi u ovom aksiomu.

Ako su A i B skupovi tada iz aksioma para slijedi egzistencija skupa $\{A, B\}$. Iz aksioma unije slijedi da je $\cup\{A, B\}$ također skup. Taj skup standardno označavamo sa $A \cup B$.

Ako su A, B i C skupovi tada iz aksioma para slijedi da postoje skupovi $\{A,\ B\}$ i $\{C\}$. Ponovnom primjenom aksioma para slijedi da postoji skup $\{\{A, B\},\ \{C\}\}$. Iz aksioma unije slijedi da postoji skup $\cup\{\{A,\ B\}, \{C\}\}$, tj. trojka $\{A,\ B,\ C\}$.

Ako je $n \in \mathbb{N}$, $n > 0$, te $A_1, \ldots, A_n$ skupovi, tada bi na sasvim analogan način dokazali da postoji skup $\{A_1, \ldots, A_n\}$. Može se pokazati da iz do sada navedenih aksioma ne slijedi egzistencija beskonačnog skupa. Kasnije ćemo navesti aksiom beskonačnosti iz kojeg će direktno slijediti egzistencija beskonačnog skupa.

Definicija 0.2. *Neka su x i y skupovi. Tada skup $\{\{x\}, \{x, y\}\}$ nazivamo uređeni par, i označavamo ga s (x, y).*

Upravo navedenu definiciju uređenog para dao je Kuratowski 1921. godine. N. Wiener je 1914. uređeni par definirao kao skup $\{\{\{x\}, \emptyset\}, \{\{y\}\}\}$.

Propozicija 0.3. *Ako vrijedi $(x_1, y_1) = (x_2, y_2)$ tada je $x_1 = x_2$ i $y_1 = y_2$.*

Dokaz. Po pretpostavci imamo $\{\{x_1\}, \{x_1, y_1\}\} = \{\{x_2\}, \{x_2, y_2\}\}$. Iz svojstava relacije jednakosti slijedi da su moguća sljedeća dva slučaja:

a) $\{x_1\} = \{x_2\}$;
Iz svojstva relacije jednakosti slijedi $x_1 = x_2$. Zatim, iz $(x_1, y_1) = (x_2, y_2)$ slijedi i $\{x_1, y_1\} = \{x_1, y_2\}$, a onda lako slijedi $y_1 = y_2$.

b) $\{x_1\} = \{x_2, y_2\}$;
Iz svojstva relacije jednakosti slijedi $x_1 = x_2$ i $x_1 = y_2$, tj. $x_1 = x_2 = y_2$. Zatim, iz $(x_1, y_1) = (x_2, y_2)$ slijedi još $\{x_1, y_1\} = \{x_2\}$. Iz svojstava relacije jednakosti slijedi opet $x_1 = y_1 = x_2$.
Iz svega prethodnog zaključujemo da je $x_1 = y_1 = x_2 = y_2$. Q.E.D.

Prije sljedeće definicije moramo istaknuti da ćemo u ovom poglavlju na intuitivnom nivou koristiti prirodne brojeve, tj. skup $\mathbb{N} = \{0, 1, 2, \ldots\}$. U sljedećem poglavlju definirat ćemo strogo skup prirodnih brojeva. Zatim, u sljedećoj definiciji koristimo rekurzivni način definiranja. Opet, u sljedećem poglavlju istaknut ćemo da su rekurzivne definicije "dozvoljene" i "dobre" u teoriji `ZF`.

Definicija 0.4. *Za svaki $n \in \mathbb{N}$, $n \geq 2$, rekurzivno definiramo uređenu n–torku ovako:*

$$(x_1, x_2) = \{\{x_1\}, \{x_1, x_2\}\}$$

$$(x_1, \ldots, x_{n+1}) = ((x_1, \ldots, x_n), x_{n+1})$$

Kako bismo mogli govoriti o Kartezijevom produktu skupova, a onda o relacijama i funkcijama, sada navodimo shemu aksioma separacije.

Shema aksioma separacije: ako je x skup i F neko zadano svojstvo[1] tada je klasa svih $z \in x$ koji imaju svojstvo F također skup, tj. formalno:

$$\forall x \exists y \forall z (z \in y \leftrightarrow (z \in x \wedge F(z)).$$

Govorimo *shema* aksioma, a ne aksiom, jer tu zapravo imamo beskonačno aksioma – za svako svojstvo F imamo po jedan aksiom.

Propozicija 0.5. *Neka su A i B skupovi. Tada je klasa $\{(x, y) : x \in A, y \in B\}$ također skup. Navedenu klasu nazivamo* **Kartezijev produkt skupova** *A i B, te je označavamo sa $A \times B$.*

Dokaz. Iz aksioma unije slijedi da postoji skup $A \cup B$. Iz aksioma partitivnog skupa slijedi da postoji skup $\mathcal{P}(\mathcal{P}(A \cup B))$. Sada iz sheme aksioma separacije slijedi da je klasa $\{z : z \in \mathcal{P}(\mathcal{P}(A \cup B)) \wedge (\exists u \in A)(\exists v \in B)(z = (u, v))\}$ skup, tj. klasa $A \times B$ je skup. Q.E.D.

Na sasvim analogan način može se dokazati da je za svaki $n \in \mathbb{N}$, $n \geq 2$, te proizvoljne skupove $A_1, \ldots, A_n$, klasa $\{(x_1, \ldots, x_n) : x_1 \in A_1, \ldots, x_n \in A_n\}$ također skup. Navedena klasa se naziva Kartezijev produkt skupova $A_1, \ldots, A_n$, te je označavamo sa $A_1 \times \ldots \times A_n$.

Primjenom sheme aksioma separacije može se pokazati da su za sve skupove A i B klase $\cap A$ i $A \setminus B$ također skupovi. Sada ćemo navedene operacije detaljno definirati.

Definicija 0.6. *Za proizvoljni skup A sa $\cap A$ označavamo klasu $\{x : za\ svaki\ y \in A\ vrijedi\ x \in y\}$, te je nazivamo* **presjek** *skupa A. Ako su A i B skupovi tada sa $A \cap B$ označavamo presjek $\cap\{A, B\}$. Analogno, ako je $n \in \mathbb{N}$, $n > 0$, te $A_1, \ldots, A_n$ skupovi, tada sa $A_1 \cap A_2 \cap \ldots \cap A_n$ označavamo presjek $\cap\{A_1, \ldots, A_n\}$.*

Propozicija 0.7. *Ako je $A \neq \emptyset$ skup tada je presjek $\cap A$ također skup.*

Definicija 0.8. *Za proizvoljne skupove A i B sa $A \setminus B$ označavamo klasu $\{x : x \in A$ i $x \notin B\}$, te je nazivamo* **razlika** *skupova A i B. Neka je U neki skup, te $A \subseteq U$. Tada sa A^c označavamo klasu $U \setminus A$, te je nazivamo komplement skupa A (u odnosu na skup U).*

Propozicija 0.9. *Za sve skupove A i B razlika $A \setminus B$ je također skup. Ako je U skup, te $A \subseteq U$, tada je komplement A^c također skup.*

Definicija 0.10. Binarna relacija *R na skupovima A i B je proizvoljni podskup Kartezijevog produkta $A \times B$. Ako su $A_1, \ldots, A_n$ skupovi tada je n–***mjesna relacija** *proizvoljni podskup Kartezijevog produkta $A_1 \times \ldots \times A_n$.*

[1] Točnije, F je proizvoljna formula teorije `ZF` s jednom slobodnom varijablom. Ovdje nećemo strogo definirati pojam formule. Grubo rečeno, formula je konačan niz znakova koji mogu biti varijable, zagrade, logički veznici, kvantifikatori, te simboli $=$ i $\in$.

Sada se nećemo baviti relacijama. Kasnije ćemo posebno promatrati relacije uređaja.

Definicija 0.11. *Neka su A i B proizvoljni skupovi, te neka je $f \subseteq A \times B$ binarna relacija koja ima svojstvo da za svaki $x \in A$ postoji jedinstveni $y \in B$ tako da vrijedi $(x, y) \in f$. Tada binarnu relaciju f nazivamo funkcija i označavamo je sa $f : A \to B$. Skup A nazivamo domena funkcije, a skup B kodomena funkcije. Ako je $f : A \to B$ funkcija, te je $(x, y) \in f$, tada umjesto y pišemo i $f(x)$.*

Funkcije možemo zadavati na razne načine. Primjerice: formulom, rekurzivno, po slučajevima, opisno, tablicom, grafom, grafikonom, ... Ako je A neki skup tada funkciju $id_A : A \to A$ zadanu sa $id_A(x) = x$ nazivamo **identiteta**. Ako je $B \subseteq A$ tada funkciju $i : B \to A$ zadanu sa $i(x) = x$ nazivamo **inkluzija**. Ako je $f : A \to B$ neka funkcija, te $C \subseteq A$ i $D \subseteq B$ tada skup $f[C] = \{f(x) : x \in C\}$ nazivamo **slika podskupa** C, odnosno skup $f^{-1}[D] = \{x \in A : f(x) \in D\}$ nazivamo **praslika podskupa** D. Slika funkcije $f : A \to B$ je tada $f[A]$. Obično sliku funkcije f označavamo sa $Rng(f)$. **Graf funkcije**[2] $f : A \to B$ je skup $\{(x, f(x)) : x \in A\}$. Kažemo da su funkcije $f : A \to B$ i $g : C \to D$ jednake, te pišemo $f = g$, ako vrijedi $A = C$, $B = D$, te za svaki $x \in A$ vrijedi $f(x) = g(x)$.

Neka su $f : A \to B$ i $g : C \to D$ funkcije takve da je $Rng(f) \subseteq C$. Tada funkciju s domenom A i kodomenom D koja svakom $x \in A$ pridružuje $g(f(x))$ nazivamo **kompozicija funkcija** f i g, te je označavamo sa $g \circ f$. Lako je provjeriti da je kompozicija funkcija asocijativna. (Je li komutativna?)

Neka je $f : A \to B$ neka funkcija, te $C \subseteq A$. Funkciju $g : C \to B$ koja je definirana sa $g(x) = f(x)$, nazivamo **restrikcija funkcije** f, te je označavamo sa $f|_C$. Kažemo još da je f **proširenje funkcije** $f|_C$.

Za funkciju $f : A \to B$ kažemo da je **injekcija** ako za sve $x_1, x_2 \in A$, takve da je $x_1 \neq x_2$, vrijedi $f(x_1) \neq f(x_2)$. Za funkciju $f : A \to B$ kažemo da je **surjekcija** ako za svaki $y \in B$ postoji $x \in A$ tako da vrijedi $y = f(x)$. Kažemo da je funkcija **bijekcija** ako je injekcija i surjekcija.

Neka je $f : A \to B$ neka funkcija. Za funkciju $g : B \to A$ kažemo da je **inverzna funkcija** od f ako vrijedi $f \circ g = id_B$ i $g \circ f = id_A$. Lako je vidjeti da ako za neku funkciju f postoji inverzna tada je ona jedinstvena. Inverznu funkciju od funkcije f označavamo sa f^{-1}. Dokažite da neka funkcija f ima inverznu ako i samo ako je f bijekcija.

Definicija 0.12. *Za svaki skup A svaki podskup $\mathcal{F}$ od $\mathcal{P}(A)$ nazivamo familija skupova. Ako su A i I neki skupovi, tada svaku funkciju $f : I \to \mathcal{P}(A)$ nazivamo indeksirana familija skupova. Obično umjesto $f(i)$ pišemo A_i, pa onda indeksiranu familiju skupova označavamo sa $(A_i : i \in I)$.*

U daljnjim izlaganjima govorit ćemo samo familija skupova, tj. nećemo posebno isticati radi li se o običnoj ili indeksiranoj familiji.

[2] Uočite da iz navedene definicije funkcije slijedi da je zapravo funkcija jednaka svom grafu.

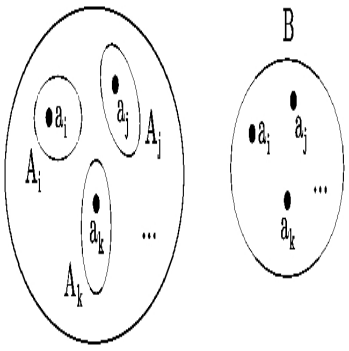
Definicija 0.13. *Neka je* $(A_i : i \in I)$ *proizvoljna familija skupova. Kartezijev produkt familije skupova, u oznaci* $\prod_{i\in I} A_i$, *definiramo kao klasu*

$$\{f|\ f : I \to \bigcup_{i\in I} A_i, \quad za\ svaki\ \ i \in I\ \ \ vrijedi\ \ \ f(i) \in A_i\}$$

Na kraju ovog uvoda navodimo još aksiom izbora. Tom aksiomu je posvećena posljednja točka drugog poglavlja. Koristit ćemo ga već prilikom nekih dokaza tvrdnji o konačnim i beskonačnim skupovima.

Aksiom izbora
Neka je $(A_i\ : i \in I)$ familija nepraznih skupova koji su u parovima disjunktni. Tada postoji skup B tako da je za svaki $i \in I$ presjek $B \cap A_i$ jednočlan skup.

Skup B nazivamo *izborni skup*. Na sljedećoj slici ilustriramo aksiom izbora (familiju skupova $(A_i : i \in I)$ i izborni skup B).



Lako je konstruirati primjer koji pokazuje da je u izreci aksioma izbora nužan uvjet da su članovi familije u parovima disjunktni.

Zadaci

1. Neka je U neki skup, te A, B i C podskupovi od U. Dokažite da vrijedi:

   (a) $(A \cap B)^c = A^c \cup B^c$
   (b) $(A \cup B)^c = A^c \cap B^c$
   (c) $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C) = (A \setminus B) \setminus C$
   (d) $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$
   (e) $A \setminus (A \setminus B) = A \cap B$
   (f) $A \cap (B \setminus C) = (A \cap B) \setminus (A \cap C) = (A \cap B) \setminus C$
   (g) $(A \cup B) \setminus C = (A \setminus C) \cup (B \setminus C)$

(h) $A^{cc} = A$

(i) $(A^c \cup B) \cap A = A \cap B$

(j) $A \cap (B \setminus A) = \emptyset$

2. Dokažite da općenito ne vrijedi $(\cap A) \cap (\cap B) = \cap(A \cap B)$.

3. Neka je $x = \{\emptyset,\ \{\emptyset\},\ \{\emptyset, \{\emptyset\}\}\}$. Napišite sljedeće skupove u obliku $\{a_1, \ldots, a_k\}$: $\bigcup x,\ \bigcap x,\ \mathcal{P}(\{x\}),\ \mathcal{P}(x) \cap \bigcup\bigcap(x,\ \{x\})$.

4. Dokažite da vrijedi:

(a) $(A \cap B) \times (C \cap D) = (A \times C) \cap (B \times D)$

(b) $\bigcap_{i \in I} A_i \times \bigcap_{i \in I} B_i = \bigcap_{i \in I}(A_i \times B_i)$

(c) $(A \times B) \cup (C \times D) \subseteq (A \cup C) \times (B \cup D)$, te odredite skupove za koje ne vrijedi jednakost

(d) $(A \cup B) \times C = (A \times C) \cup (B \times C)$

(e) $A \times (B \cup C) = (A \times B) \cup (A \times C)$

(f) $(A \cup B) \times (C \cup D) = (A \times C) \cup (B \times C) \cup (A \times D) \cup (B \times D)$

(g) $(A \setminus B) \times C = (A \times C) \setminus (B \times C)$

(h) $A \times (B \setminus C) = (A \times B) \setminus (A \times C)$

(i) $A \times B = (A \times D) \cap (C \times D)$, gdje je $A \subseteq C$ i $B \subseteq D$

(j) $U^2 \setminus (A \times B) = [(U \setminus A) \times U] \cup [U \times (U \setminus B)]$

(k) $\bigcup_{i \in I} A_i \times \bigcup_{j \in J} B_j = \bigcup_{(i,j) \in I \times J} (A_i \times B_j)$

(l) $\bigcap_{i \in I} A_i \times \bigcap_{j \in J} B_j = \bigcap_{(i,j) \in I \times J} (A_i \times B_j)$

(m) ako je $A, B \neq \emptyset$ i $(A \times B) \cup (B \times A) = C \times D$ tada je $A = B = C = D$

5. Operacija simetrične razlike Δ definirana je za proizvoljne skupove A i B ovako: $A \Delta B = (A \setminus B) \cup (B \setminus A)$. Dokažite da vrijedi:

(a) $A \Delta B = B \Delta A$

(b) ako $A \Delta B = A \Delta C$ tada $B = C$

(c) $A \cap (B \Delta C) = (A \cap B) \Delta (A \cap C)$

(d) $A \Delta (B \Delta C) = (A \Delta B) \Delta C$

(e) $A \cap (B \Delta C) = (A \cap B) \Delta (A \cap C)$

(f) $A \cup B = (A \Delta B) \Delta (A \cap B) = (A \Delta B) \cup (A \cap B)$

(g) $A \setminus B = A\Delta(A \cap B)$

(h) $A\Delta B = A^c \Delta B^c$

(i) $C = A\Delta B$ ako i samo ako $A = B\Delta C$

6. Vrijedi li općenito:

(a) $\mathcal{P}(a) \cap \mathcal{P}(b) = \mathcal{P}(a \cap b)$?

(b) $\mathcal{P}(a) \setminus \mathcal{P}(b) = \mathcal{P}(a \setminus b)$?

(c) $\mathcal{P}(a) \cup \mathcal{P}(b) = \mathcal{P}(a \cup b)$?

(d) $a \in b$ ekvivalentno s $\mathcal{P}(a) \in \mathcal{P}(b)$?

(e) $\mathcal{P}(a) = \mathcal{P}(b)$ ako i samo ako $a = b$?

Rješenje.

(a) Vrijedi. Za proizvoljan x, dokažimo da je $x \in \mathcal{P}(a) \cap \mathcal{P}(b) \leftrightarrow x \in \mathcal{P}(a \cap b)$. To se naravno svodi na $x \subseteq a \wedge x \subseteq b \leftrightarrow x \subseteq a \cap b$, što se lako dokaže.

(b) Ne vrijedi (nikada), jer $\emptyset \in \mathcal{P}(x)$ za svaki skup x. Dakle $\emptyset$ je element desne strane, a nije element lijeve.

(c) Općenito ne vrijedi. Primjerice za $a = \{1\}$ i $b = \{2\}$. Ponekad jest, primjerice kad je $a \subseteq b$.

(d) Jedan smjer vrijedi: ako je $\mathcal{P}(a) \in \mathcal{P}(b)$, to znači $\mathcal{P}(a) \subseteq b$, pa su svi elementi od $\mathcal{P}(a)$ ujedno u b. Budući da je $a \in \mathcal{P}(a)$, vrijedi $a \in b$. Drugi smjer ne vrijedi na primjer za $a = \{1\}$ i $b = \{\{1\}\}$.

(e) Vrijedi.

7. Dokažite da vrijedi:

(a) $\mathcal{P}(\bigcap_{i \in I} A_i) = \bigcap_{i \in I} \mathcal{P}(A_i)$

(b) $\mathcal{P}(A \cup B) = \{A_1 \cup B_1 : A_1 \subseteq A \text{ i } B_1 \subseteq B\}$

(c) $\mathcal{P}(\bigcup_{i \in I} A_i) = \{\bigcup_{i \in I} B_i : B_i \in \mathcal{P}(A_i)\}$

8. Dokažite da za svaki skup a vrijedi $\{\emptyset, \{\emptyset\}\} \in \mathcal{PPP}(a)$.
Rješenje. Znamo $\emptyset \in \mathcal{P}(x)$, za svaki skup x. Dakle specijalno $\emptyset \in \mathcal{P}(a)$. To znači $\{\emptyset\} \subseteq \mathcal{P}(a)$ (jer su svi njegovi elementi u $\mathcal{P}(a)$), odnosno $\{\emptyset\} \in \mathcal{PP}(a)$. Također iz $\emptyset \in \mathcal{P}(y)$ za $y = \mathcal{P}(a)$ imamo $\emptyset \in \mathcal{PP}(a)$, što zajedno s gornjim daje da su svi elementi od $\{\emptyset, \{\emptyset\}\}$ u $\mathcal{PP}(a)$. Dakle, $\{\emptyset, \{\emptyset\}\}$ je podskup od $\mathcal{PP}(a)$, odnosno element od $\mathcal{PPP}(a)$.

9. Odredite $\mathcal{P}(\emptyset) \cap \mathcal{PP}(\emptyset) \cap \mathcal{PPP}(\emptyset)$.
   Rješenje. Budući da je prvi operand $\mathcal{P}(\emptyset) = \{\emptyset\}$, a $\emptyset$ se, znamo, nalazi i u ostalim partitivnim skupovima, presjek je upravo $\{\emptyset\}$.

10. Dokažite da za svaka dva skupa A i B vrijedi ${}^{B}A \subseteq \mathcal{PPPP}(A \cup B)$.

11. Neka je $(A_i : i \in I)$ proizvoljna familija skupova. Dokažite da tada vrijedi:

$$\prod_{i \in I} A_i \in \mathcal{PPPP}(I \cup \cup_{i \in I} A_i)$$

12. Neka su x i y proizvoljni skupovi. Dokažite da vrijedi:

    (a) $\bigcup\bigcap(x, y) = \bigcup(\{x\} \cap \{x, y\}) = \bigcup\{x\} = x$
    (b) $\bigcap\bigcup(x, y) = \bigcap\{x, y\} = x \cap y$
    (c) $\bigcup\bigcup(x, y) = x \cup y$
    (d) $\bigcap\bigcup(x, y) \cup (\bigcup\bigcup(x, y) \setminus \bigcup\bigcap(x, y)) =$
    $= (x \cap y) \cup ((x \cup y) \setminus x) = (y \cap x) \cup (y \setminus x) = y$

13. Koji od sljedećih skupova $[x, y]$ imaju svojstvo uređenog para, tj. vrijedi

$$[x, y] = [x', y'] \qquad \text{ako i samo ako} \qquad x = x' \text{ i } y = y',$$

    ako definiramo redom:

    (a) $[x, y] = \{\{x, y\}, \{y\}\}$;
    (b) $[x, y] = \{x, \{y\}\}$;
    (c) $[x, y] = \{x, \{x, y\}\}$.

14. Neka je $f : S \to T$ proizvoljna funkcija, te $A, B \subseteq S$ i $C, D \subseteq T$. Dokažite da vrijedi:

    (a) ako $A \subseteq B$ tada je $f[A] \subseteq f[B]$;
    (b) $f[A \cup B] = f[A] \cup f[B]$;
    (c) $f[A \cap B] \subseteq f[A] \cap f[B]$, te navedite primjer koji pokazuje da općenito ne vrijedi obrnuta inkluzija;
    (d) ako $C \subseteq D$ tada je $f^{-1}[C] \subseteq f^{-1}[D]$;
    (e) $f^{-1}[C \cap D] = f^{-1}[C] \cap f^{-1}[D]$;
    (f) $f^{-1}[C \cup D] = f^{-1}[C] \cup f^{-1}[D]$;
    (g) $f[A \setminus B] \supseteq f[A] \setminus f[B]$, te navedite primjer koji pokazuje da općenito ne vrijedi obrnuta inkluzija;

(h) $f^{-1}[C \setminus D] = f^{-1}[C] \setminus f^{-1}[D]$;

(i) $A \subseteq f^{-1}[f[A]]$, te navedite primjer koji pokazuje da općenito ne vrijedi obrnuta inkluzija;

(j) $f[A] \cap C = f[A \cap f^{-1}[C]]$;

(k) $f[A] \subseteq C$ ako i samo ako $A \subseteq f^{-1}[C]$.

15. Neka je $f : A \to B$ injekcija. Ako je $(X_i : i \in I)$ neka familija podskupova skupa A dokažite da je tada $f[\bigcap_{i \in I} X_i] = \bigcap_{i \in I} f[X_i]$. Zatim, dokažite da za sve $X_1, X_2 \subseteq A$ vrijedi $f[X_1 \setminus X_2] = f[X_1] \setminus f[X_2]$.

16. Neka su $f : A \to B$ i $g : C \to D$ funkcije takve da je definirana kompozicija $g \circ f$. Dokažite:

(a) ako je $g \circ f$ injekcija tada je i f injekcija;

(b) ako je $g \circ f$ surjekcija tada je i g surjekcija;

(c) ako je $g \circ f$ bijekcija tada je f injekcija, a g surjekcija.

17. Dokažite da je konstantna funkcija bijekcija ako samo ako su joj domena i kodomena jednočlani skupovi.

Poglavlje 1

Naivna teorija skupova

Kako bismo mogli opravdati uvođenje daljnjih aksioma teorije skupova, te ih dobro motivirati, moramo prvo naučiti još neke činjenice o skupovima. Sjetimo se da je naš glavni cilj definirati kumulativnu hijerarhiju, odnosno definirati što znači pojam "nivoa" – točnije ordinalnog broja (na taj način ćemo odgovoriti na pitanje što je skup). Pošto to nećemo raditi tako da se uvijek strogo pozivamo na aksiome onda se taj dio teorije naziva naivna teorija skupova.

Ovo poglavlje se sastoji od osam točaka. U prvim točkama prvo se bavimo "veličinom" skupova, tj. razmatramo pojmove kao što su ekvipotentni skupovi, konačni i beskonačni skupovi, prebrojivi i neprebrojivi skupovi, te kardinalnost. U sljedećim točkama razmatramo pojmove kao što su parcijalno, linearno i dobro uređeni skupovi. To nam je motivacija za definiciju nivoa u kumulativnoj hijerarhiji.

1.1 Ekvipotentni skupovi

Nije pretjerano reći da čitavu matematiku prožima ideja beskonačnosti. Sjetimo se beskonačnih skupova s kojima ste se već susreli u osnovnoj i srednjoj školi. To su prije svega skupovi brojeva: prirodnih, cijelih, racionalnih, realnih i kompleksnih. Zatim, u geometriji se govori o skupu svih točaka ravnine, skupu svih dužina, skupu svih pravaca, ... Svi ti skupovi su beskonačni.

Jedan moj profesor je u šali rekao da bi matematičari mogli zatvoriti dućan da nema beskonačnosti.

Sjetimo se kako smo kao mali učili brojati predmete – uspostavljanje bijekcije između prstiju na ruci i predmeta. Cantor je tu ideju proširio i na beskonačne skupove.

Jedna od osnovnih Cantorovih ideja o jednakobrojnim skupovima je nevjerojatno jednostavna: za dva skupa A i B kažemo da su jednakobrojni ili ekvipotentni ako postoji bijekcija $f : A \to B$. No, moramo imati na umu da ni genijalni grčki matematičari, a ni svi poslije njih sve do Cantora, nisu uočili "različite" beskonačne skupove. Na primjer skup realnih brojeva $\mathbb{R}$ ima "više" elemenata nego skup prirodnih brojeva $\mathbb{N}$, tj. ne postoji bijekcija između $\mathbb{R}$ i $\mathbb{N}$. No, skup $\mathbb{N}$ je ekvipotentan sa skupom svih parnih prirodnih brojeva, te sa skupom cijelih, a i skupom svih racionalnih brojeva.

Definicija 1.1. *Kažemo da su skupovi A i B* **ekvipotentni** *ako postoji barem jedna bijekcija $f : A \to B$. Oznaka: $A \sim B$.*

Primjer 1.2. *a)* $\{2, 7, 19\} \sim \{153, 1001, 10^{12}\}$;

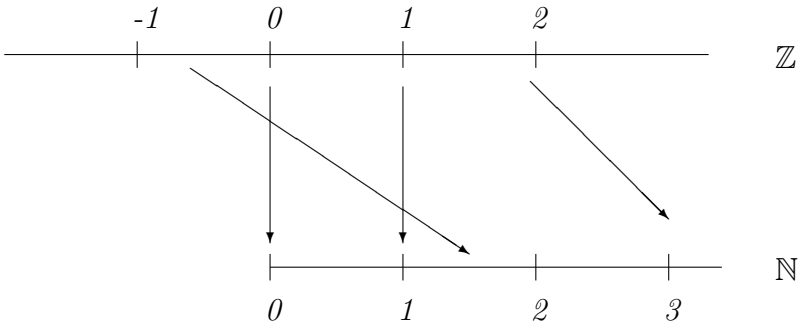
b) $\{1, 2, 3, \ldots\} \sim \{-1, -2, -3, \ldots\}$;

c) $\{1, 2, 3, \ldots\} \sim \{1, 3, 5, \ldots\}$; *jedna bijekcija je dana sa* $n \mapsto 2n - 1$

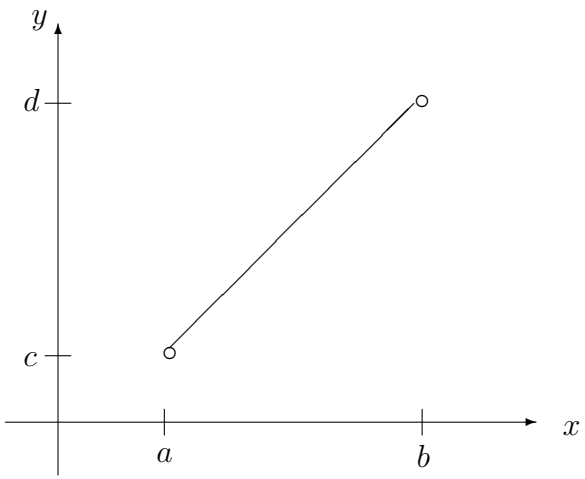
d) $\mathbb{N} \sim \mathbb{Z}$; *jedna bijekcija* $f : \mathbb{Z} \to \mathbb{N}$ *je dana sa:*

$$f(x) = \begin{cases} -2x, & \text{ako je } x < 0; \\ 0, & \text{ako je } x = 0; \\ 2x - 1, & \text{ako je } x > 0 \end{cases}$$

Upravo definiranu bijekciju ilustriramo na sljedećoj slici.



e) Svi zatvoreni segmenti realnih brojeva su međusobno ekvipotentni. Jedna bijekcija $f : [a, b] \to [c, d]$ *je dana sa* $f(x) = \dfrac{d - c}{b - a}(x - a) + c$. *Na sljedećoj slici ilustriramo kako smo dobili navedenu bijekciju (jednadžba pravca kroz dvije točke).*



Primjer 1.3. Hilbertov hotel. *Zamislimo da negdje daleko u Svemiru postoji hotel s beskonačno mnogo soba. Sobe su numerirane brojevima 1, 2, 3, ... No, zamislimo da su sve sobe zauzete gostima, i dolazi još jedan putnik koji želi sobu. Što će portir napraviti s njim? Jednostavno, zamolit će gosta iz sobe 1 da se premjesti u sobu 2, gost iz sobe 2 u sobu 3, itd. Novopridošlog gosta će tada smjestiti u sobu broj 1. (Nemojte si postavljati pitanje koliko će to premještanje trajati!)*

Pokušajte sami odgovoriti što će portir napraviti kada stigne 1000 novih gostiju, a sve sobe hotela su pune.

Promotrimo još jedan problem s kojim bi se mogao susresti portir hotela s beskonačno mnogo soba, i čije sve sobe su pune. Zamislimo da u Svemiru postoji još jedan hotel s beskonačno mnogo soba čije su sve sobe popunjene gostima. Jednog dana glavna komisija za graditeljstvo u svemirskim prostranstvima otkrila je da taj drugi hotel nema građevinsku dozvolu. Istog trena taj drugi hotel je morao biti zatvoren i svi gosti (beskonačno mnogo njih!) stali su pred vrata prvog hotela (čije su sve sobe pune). No, portir se brzo snašao. Gosta iz sobe 1 svojeg hotela premjestio je u sobu 2, gosta iz sobe 2 u sobu 4, gosta iz sobe 3 u sobu 6, itd. Tako je ispraznio sve sobe s neparnim brojevima, te je u njih smjestio goste iz zatvorenog hotela.

Sada kada se već tako dobro snalazimo s hotelima s beskonačno mnogo soba promotrimo još jedan problem koji bi portiru mogao zadati mnogo glavobolja. Zamislimo da u Svemiru postoji beskonačno mnogo hotela s beskonačno mnogo soba, i sve su sobe popunjene gostima. Svemirska građevinska komisija iz raznih je razloga zatvorila sve hotele osim jednog. Tada su svi gosti (po beskonačno mnogo njih iz svakog od beskonačno mnogo hotela) došli pred vrata tog jednog hotela koji je još imao dozvolu za rad. Snalažljivi portir sada nije znao rješenje ove na prvi pogled bezizlazne situacije. Trebao je pomoć matematičara. Može li se uopće ova ogromna grupa novopridošlih gostiju smjestiti u (puni!) hotel? Možete li pomoći portiru?

Više detalja o Hilbertovom hotelu možete pronaći u [37].

1.2 Konačni i beskonačni skupovi

U ovim izlaganjima koristimo skup $\mathbb{N}$ na intuitivnom nivou, tj. pretpostavljamo da su nam poznata svojstva klase $\{0,\ 1,\ 2,\ \ldots\}$, koju nazivamo skup prirodnih brojeva, te je označavamo sa $\mathbb{N}$.

Za svaki $k \in \mathbb{N} \setminus \{0\}$ sa $\mathbb{N}_k$ označavamo skup $\{1, \ldots, k\}$, a $\mathbb{N}_0$ je prazan skup.

Teorem 1.4. *Neka je $k \in \mathbb{N}$ proizvoljan. Ako je $f : \mathbb{N}_k \to \mathbb{N}_k$ injekcija tada je f i surjekcija.*

Dokaz. Indukcijom po k dokazuje se da je svaka injekcija $f : \mathbb{N}_k \to \mathbb{N}_k$ ujedno i surjekcija. Za detalje vidite zadatak 1 na stranici 23.

Definicija 1.5. *Kažemo da je skup A* **konačan** *ako postoji $k \in \mathbb{N}$ tako da je skup A ekvipotentan sa skupom $\mathbb{N}_k$.*

Napomena 1.6. *Iz teorema 1.4. slijedi da za svaki konačan skup A postoji jedinstveni $k \in \mathbb{N}$ takav da vrijedi $A \sim \mathbb{N}_k$. To nam omogućava da za svaki konačan skup A definiramo broj elemenata, u oznaci $k(A)$, stavljajući $k(A) = n$, pri čemu vrijedi $A \sim \mathbb{N}_n$.*

Dokaz sljedećeg teorema dan je kao rješenje zadatka 2 na stranici 24.

Teorem 1.7. *Za svaki $A \subseteq \mathbb{N}_m$ postoji prirodan broj k takav da vrijedi $k \leq m$ i $k(A) = k$.*

Korolar 1.8. *Svaki podskup konačnog skupa je konačan.*

Teorem 1.9. *Skup X je konačan ako i samo ako postoji $k \in \mathbb{N}$ i surjekcija $f : \mathbb{N}_k \to X$.*

Za dokaz vidite rješenje zadatka 5 na stranici 24.

Definicija 1.10. *Za skup X kažemo da je* **beskonačan** *ako nije konačan.*

Kao što smo već više puta istaknuli u ovom poglavlju razmatramo naivnu teoriju skupova, te nam je cilj istaknuti činjenice koje koristimo u dokazima. Dokaz sljedeće leme dan je kao rješenje zadatka 6. Želimo istaknuti da se u dokazu leme koriste pojmovi o uređenim skupovima, te se koristi Zornova lema, za koju se kasnije dokazuje da je ekvivalentna aksiomu izbora.

Lema 1.11. *Za svaki beskonačan skup X postoji injekcija $f : \mathbb{N} \to X$.*

Teorem 1.12. *Neka je X neki skup. Sljedeće tvrdnje su ekvivalentne:*

a) skup X je beskonačan;

b) postoji injekcija iz $\mathbb{N}$ *u* X;

c) postoji injekcija iz X *u* X *koja nije surjekcija;*

d) skup X *je ekvipotentan s nekim svojim pravim podskupom.*

Dokaz prethodnog teorema dan je kao rješenje zadatka 7 na stranici 25.

Korolar 1.13. *Skup* X *je konačan ako i samo ako je svaka injekcija iz* X *u* X *ujedno i surjekcija.*

Dokaz. Iz prethodnog teorema posebno imamo $a) \Leftrightarrow c)$, a onda i $\neg\ a) \Leftrightarrow \neg\ c)$. Q.E.D.

Zadaci

1. Neka je $k \in \mathbb{N}$ proizvoljan. Dokažite da ako je $f : \mathbb{N}_k \to \mathbb{N}_k$ injekcija tada je f i surjekcija.
   Dokaz. Indukcijom po k dokazujemo da je svaka injekcija $f : \mathbb{N}_k \to \mathbb{N}_k$ ujedno i surjekcija. Ako je $k = 0$ tvrdnja je trivijalno isitinita. Ako je $k = 1$ tada je očito funkcija $f : \{1\} \to \{1\}$ surjekcija. Neka je $k \in \mathbb{N} \setminus \{0\}$ prirodan broj koji ima svojstvo da je svaka injekcija $g : \mathbb{N}_k \to \mathbb{N}_k$ ujedno i surjekcija. Neka je $f : \mathbb{N}_{k+1} \to \mathbb{N}_{k+1}$ proizvoljna injekcija. Tada je restrikcija $f|_{\mathbb{N}_k} : \mathbb{N}_k \to \mathbb{N}_{k+1}$ također injekcija. Sada razlikujemo dva slučaja:

   a) $f(k+1) = k+1$
      To znači da je slika restrikcije $f|_{\mathbb{N}_k}$ sadržana u skupu $\mathbb{N}_k$. Time imamo da je funkcija $f|_{\mathbb{N}_k} : \mathbb{N}_k \to \mathbb{N}_k$ injekcija. Iz pretpostavke indukcije slijedi da je ta funkcija surjekcija. Sada je očito da je funkcija f surjekcija.

   b) $f(k+1) = i_0 \in \mathbb{N}_k$
      Primijetimo prvo da postoji $j_0 \in \mathbb{N}_k$ takav da je $f(j_0) = k+1$ (Pretpostavimo da takav $j_0 \in \mathbb{N}_k$ ne postoji. Tada je restrikcija $f|_{\mathbb{N}_k} : \mathbb{N}_k \to \mathbb{N}_k$ dobro definirana, te je injekcija. Iz pretpostavke indukcije slijedi da je ta restrikcija i surjekcija. No, tada postoji neki $i_1 \in \mathbb{N}_k$ takav da je $f(i_1) = i_0$. Time imamo $f(k+1) = f(i_1)$, te $k+1 \neq i_1$, što je kontradikcija s pretpostavkom da je funkcija $f : \mathbb{N}_{k+1} \to \mathbb{N}_{k+1}$ injekcija).
      Definiramo funkciju $F : \mathbb{N}_k \to \mathbb{N}_k$ ovako:

$$F(x) = \begin{cases} f(x), & \text{ako je } x \neq j_0; \\ i_0, & \text{ako je } x = j_0. \end{cases}$$

   Očito je funkcija $F : \mathbb{N}_k \to \mathbb{N}_k$ injekcija. Iz pretpostavke indukcije slijedi da je ta funkcija i surjekcija. Sada je lako vidjeti da iz toga slijedi da je i funkcija f surjekcija (Neka je $y \in \mathbb{N}_{k+1}$ proizvoljan. Razlikujemo tri slučaja. Ako je

$y \in \mathbb{N}_k \setminus \{i_0\}$ tada iz surjektivnosti funkcije F i njene definicije slijedi da postoji $x \in \mathbb{N}_k$ takav da je $f(x) = y$. Ako je $y = i_0$ tada imamo $f(k+1) = i_0$. Ako je $y = k+1$ tada imamo $f(j_0) = k+1$).

2. Dokažite da za svaki podskup $A \subseteq \mathbb{N}_m$ postoji prirodan broj k takav da vrijedi $k \leq m$ i $k(A) = k$.
Dokaz. Indukcijom po m. Ako je $m = 0$ ili $m = 1$ tvrdnja očito vrijedi. Neka je $m \in \mathbb{N}$ takav da za svaki podskup B od $\mathbb{N}_m$ postoji $k \leq m$ takav da je $k(B) = k$. Neka je A proizvoljan podskup od $\mathbb{N}_{m+1}$. Ako je $A \subseteq \mathbb{N}_m$ tvrdnja slijedi iz pretpostavke indukcije. Promotrimo slučaj kada je $m+1 \in A$. Tada je $A \setminus \{m+1\} \subseteq \mathbb{N}_m$. Iz pretpostavke indukcije slijedi da postoji $k \in \mathbb{N}$ takav da je $k(A \setminus \{m+1\}) = k$. Tada je očito $k(A) = k+1$.

3. Dokažite da je svaki podskup konačnog skupa konačan.
Dokaz. Neka je X proizvoljan konačan skup, te A njegov proizvoljan podskup. Ako je $A = \emptyset$ tada je A konačan po definiciji. Promatramo slučaj kada je $A \neq \emptyset$. Budući da je i skup X konačan, tada po definiciji postoji $m > 0$ takav da je $X \sim \mathbb{N}_m$. Neka je $f : X \to \mathbb{N}_m$ neka bijekcija. Promotrimo restrikciju $f|_A$. Ta funkcija je očito injekcija, te vrijedi $k(A) = k(f[A])$. Budući da je $f[A] \subseteq \mathbb{N}_m$ tada iz prethodnog zadatka slijedi da postoji $k \leq m$ takav da je $k(f[A]) = k$. Tada je $k(A) = k$, pa je skup A konačan.

4. Dokažite da je skup koji ima beskonačan podskup također beskonačan.

5. Dokažite da je skup X konačan ako i samo ako postoji $k \in \mathbb{N}$ i surjekcija $f : \mathbb{N}_k \to X$.
Dokaz. Pretpostavimo prvo da je skup X konačan. Tada iz definicije slijedi da postoji $k \in \mathbb{N}$ i bijekcija $f : X \to \mathbb{N}_k$. Tada je f^{-1} jedna tražena surjekcija.

   Pretpostavimo sada da postoji $k \in \mathbb{N}$ i surjekcija $f : \mathbb{N}_k \to X$. Tada očito za svaki $x \in X$ imamo $f^{-1}[\{x\}] \neq \emptyset$. Primjenom aksioma izbora slijedi da za svaki $x \in X$ možemo odabrati po jedan $a_x \in f^{-1}[\{x\}]$. Označimo $A = \{a_x \ : \ x \in X\}$. Očito je $A \subseteq \mathbb{N}_k$, te je funkcija $g : A \to X$, koja je definirana sa $g(a_x) = x$, bijekcija. Tada je $k(A) = k(X)$. Iz $A \subseteq \mathbb{N}_k$ i zadatka 2 slijedi da postoji $m \leq k$ takav da je $k(A) = m$. Tada je $k(X) = m$, te je skup X konačan.

6. * Dokažite lemu 1.11.
Dokaz. U dokazu leme koristimo Zornovu lemu koju razmatramo na strani 90. Za iskaz Zornove leme, a i u ovom dokazu, koriste se neki pojmovi o uređenim skupovima. Svi ti pojmovi su definirani u jednoj od sljedećih točaka.

   Neka je X beskonačan skup. Neka je S skup svih konačnih nizova $(x_0, x_1, \ldots, x_n)$ elemenata od X, pri čemu je $x_i \neq x_j$, za sve $i \neq j$. Na skupu S definiramo parcijalni uređaj ovako:

   $(x_0, x_1, \ldots, x_n) < (y_0, y_1, \ldots, y_m)$, ako $n < m$, te vrijedi $x_i = y_i$ za sve $i \leq n$

Pošto je X beskonačan, očito skup S ne sadrži maksimalni element. Iz toga slijedi da skup S ne ispunjava uvjete Zornove leme. Neka je $L \subseteq S$ neki lanac za koji ne postoji gornja međa u S. Lako je vidjeti da je sa $k \mapsto x_k$, gdje je $(x_0, x_1, \ldots, x_n) \in L$ i $k \leq n$, definirana jedna injekcija sa $\mathbb{N}$ u skup X.

7. Dokažite teorem 1.12.
Dokaz.

$a \Rightarrow b)$ To je dokazano u lemi 1.11.

$b) \Rightarrow c)$ Neka je $f : \mathbb{N} \to X$ neka injekcija. Definiramo funkciju $g : X \to X$ ovako:

$$g(x) = \begin{cases} x, & x \notin f[\mathbb{N}]; \\ \\ f(n+1), & x = f(n). \end{cases}$$

Pokažimo da je funkcija g injekcija. Neka su $x_1,\ x_2 \in X$ takvi da je $x_1 \neq x_2$. Razlikujemo tri slučaja:

(i) $x_1,\ x_2 \notin f[\mathbb{N}]$. Tada je $g(x_1) = x_1 \neq x_2 = g(x_2)$.

(ii) $x_1 \in f[\mathbb{N}]$ i $x_2 \notin f[\mathbb{N}]$. Tada je $g(x_1) \in f[\mathbb{N}]$, a $g(x_2) \notin f[\mathbb{N}]$, pa je očito $g(x_1) \neq g(x_2)$.

(iii) $x_1,\ x_2 \in f[\mathbb{N}]$. Tada je $x_1 = f(n)$ i $x_2 = f(m)$, za neke $n, m \in \mathbb{N}$. Pošto je $x_1 \neq x_2$ tada je $n \neq m$. No, funkcija f je po pretpostavci injekcija, pa je $f(n+1) \neq f(m+1)$, a onda je $g(x_1) \neq g(x_2)$.

Funkcija g nije surjekcija jer $f(0) \in X \setminus g(X)$.

$c) \Rightarrow d)$ Neka je $f : X \to X$ neka injekcija koja nije surjekcija. Tada je $f[X]$ pravi podskup od X, te je očito $f : X \to f[X]$ bijekcija. To znači da vrijedi $X \sim f(X)$.

$d) \Rightarrow a)$ Neka je $Y \subset X$ i $g : X \to Y$ bijekcija. Pretpostavimo da je skup X konačan. Tada iz definicije slijedi da postoji $k \in \mathbb{N}$ takav da je $X \sim \mathbb{N}_k$. Neka je $f : \mathbb{N}_k \to X$ jedna bijekcija. Tada je $h = f^{-1} \circ g \circ f : \mathbb{N}_k \to \mathbb{N}_k$ injekcija. No, $h[\mathbb{N}_k] = f^{-1}[g[f[\mathbb{N}_k]]] = f^{-1}[g[X]] = f^{-1}[Y] \neq \mathbb{N}_k$, pa h nije surjekcija. To je u kontradikciji s teoremom 1.4.

1.3 Prebrojivi skupovi

U ovoj točki razmatrat ćemo beskonačne skupove koji imaju najmanje moguće elemenata, tj. njihova beskonačnost je najmanja moguća.

Definicija 1.14. *Za skup kažemo da je* **prebrojiv** *ako je ekvipotentan sa skupom* $\mathbb{N}$. *Ako je skup beskonačan i nije prebrojiv tada kažemo da je* **neprebrojiv**.

Primjer 1.15. *Skup* $\mathbb{N}$ *je prebrojiv jer je* $id : \mathbb{N} \to \mathbb{N},\ id(x) = x$, *bijekcija.*

Skup $2\mathbb{N}$ *svih parnih prirodnih brojeva je prebrojiv jer je* $f : \mathbb{N} \to 2\mathbb{N}$, $f(x) = 2x$, *jedna bijekcija.*

Skup $2\mathbb{N} + 1$ *svih neparnih prirodnih brojeva je prebrojiv jer je* $f : \mathbb{N} \to 2\mathbb{N} + 1$, $f(x) = 2x + 1$, *jedna bijekcija.*

Skup $\mathbb{Z}$ *svih cijelih brojeva je prebrojiv jer postoji bijekcija između skupa* $\mathbb{Z}$ *i skupa* $\mathbb{N}$. *Jednu bijekciju smo naveli na strani 20 u primjeru 1.2.*

Nije teško pokazati da su i sljedeći skupovi prebrojivi:

- *Skup svih točaka ravnine s racionalnim koordinatama;*
- *Skup svih intervala realnih brojeva s racionalnim krajevima;*
- *Skup svih polinoma nad poljem racionalnih brojeva;*
- *Skup svih algebarskih realnih brojeva.*

Dokazi prebrojivosti navedenih skupova dani su u [4].

Sada nam je cilj dokazati da je prebrojiva unija prebrojivih skupova ponovno prebrojiv skup. Tada ćemo kao jednostavnu posljedicu dobiti da je skup $\mathbb{Q}$ prebrojiv.

Propozicija 1.16. *Neka je* $(B_j : j \in \mathbb{N})$ *familija skupova koja ima svojstvo da je za svaki* $j \in \mathbb{N}$ *skup* B_j *konačan, te su članovi familije u parovima disjunktni. Tada je skup* $\bigcup_{j\in\mathbb{N}} B_j$ *konačan ili prebrojiv.*

Dokaz. Pretpostavimo da skup $\bigcup_{j\in\mathbb{N}} B_j$ nije konačan. Za svaki $j \in \mathbb{N}$ označimo sa $k(B_j)$ broj elemenata skupa B_j (iz točke o konačnim skupovima slijedi da je taj pojam dobro definiran; vidi napomenu 1.6.). Neka je $I = \{j : B_j \neq \emptyset\}$. Za svaki $j \in I$ sa A_j označimo skup svih bijekcija između skupova B_j i $\mathbb{N}_{k(B_j)}$. Očito je $(A_j : j \in I)$ neprazna familija nepraznih skupova koji su u parovima disjunktni. Iz aksioma izbora slijedi da postoji skup B tako da je $B \cap A_j$ jednočlan skup za svaki $j \in \mathbb{N}$. Za svaki $j \in \mathbb{N}$ neka je $\{f_j\} = B \cap A_j$. Sada definiramo funkciju $f : \bigcup_{j\in\mathbb{N}} B_j \to \mathbb{N}$ ovako: ako je $x \in \bigcup_{j\in\mathbb{N}} B_j$ tada postoji jedinstveni $j_0 \in \mathbb{N}$ takav da je $x \in B_{j_0}$, pa onda neka je $f(x) = \sum_{j<j_0} k(B_j) + f_{j_0}(x) - 1$. Funkcija f je očito bijekcija. Q.E.D.

Propozicija 1.17. *Neka je* $(B_j : j \in \mathbb{N})$ *familija skupova koja ima svojstvo da je za svaki* $j \in \mathbb{N}$ *skup* B_j *konačan. Tada je skup* $\bigcup_{j\in\mathbb{N}} B_j$ *konačan ili prebrojiv. (Za razliku od prethodne propozicije ovdje ne pretpostavljamo da su članovi familije u parovima disjunktni).*

Dokaz prethodne propozicije dan je kao rješenje zadatka 1 na strani 30.

Lema 1.18. *Neka je A konačan, a B prebrojiv skup. Tada je skup $A \cup B$ prebrojiv.*

Dokaz prethodne leme dan je kao rješenje zadatka 2 na strani 30.

Propozicija 1.19. *Neka je $n \in \mathbb{N} \setminus \{0\}$, proizvoljan, te neka su $A_0, \ldots, A_{n-1}$ prebrojivi skupovi koji su u parovima disjunktni. Tada je skup $A_0 \cup \ldots \cup A_{n-1}$ također prebrojiv.*

Dokaz prethodne propozicije dan je kao rješenje zadatka 3 na strani 30. Uočite da u dokazu prethodne propozicije nije korišten aksiom izbora. O (ne)nužnosti korištenja AC u dokazima možete čitati u [39].

Propozicija 1.20. *Neka je $(A_j : j \in \mathbb{N})$ familija skupova čiji su elementi u parovima disjunktni prebrojivi skupovi. Tada je skup $\bigcup_{j\in\mathbb{N}} A_j$ prebrojiv.*

Dokaz. Neka je $B_0 = \{0,\ 1,\ 3,\ 5,\ 7,\ \ldots\}$, a za svaki $j \in \mathbb{N} \setminus \{0\}$ neka je $B_j = \{(2i+1) \cdot 2^j : i \in \mathbb{N}\}$. Lako je vidjeti da vrijedi:

a) za svaki $j \in \mathbb{N}$ skup B_j je prebrojiv;

b) za sve $i \neq j$ vrijedi $B_i \cap B_j = \emptyset$;

c) $\bigcup_{j\in\mathbb{N}} B_j = \mathbb{N}$;

d) za svaki $j \in \mathbb{N}$ vrijedi $A_j \sim B_j$.

Za svaki $j \in \mathbb{N}$ označimo sa $\mathcal{A}_j$ skup svih bijekcija između A_j i B_j. Iz aksioma izbora slijedi da postoji skup $\mathcal{B}$ tako da je za svaki $j \in \mathbb{N}$ skup $\mathcal{B} \cap \mathcal{A}_j$ jednočlan. Za svaki $j \in \mathbb{N}$ označimo sa f_j jedinstvenu funkciju za koju vrijedi $\mathcal{B} \cap \mathcal{A}_j = \{f_j\}$.

Sada definiramo $f : \bigcup_{j\in\mathbb{N}} A_j \to \mathbb{N}$ tako da vrijedi $f|_{A_j} = f_j$. Očito je funkcija f bijekcija. Q.E.D.

Napomena 1.21. *Prethodnu propoziciju možemo dokazati i* **dijagonalnim postupkom** [1]. *To ćemo sada kratko skicirati. Pošto je svaki skup A_k prebrojiv možemo njegove elemente poredati u niz. Time imamo:*

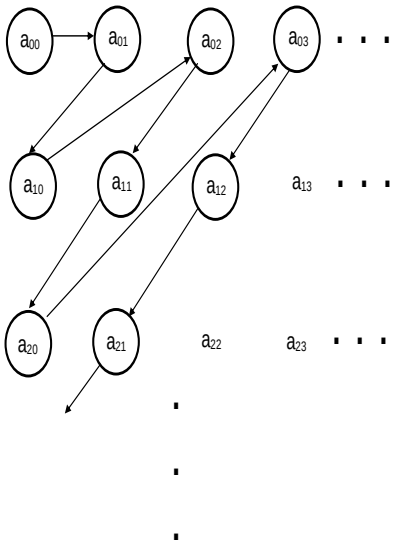
$$\begin{array}{cccccccc}
A_0 & \ldots & a_{00} & a_{01} & a_{02} & a_{03} & \ldots \\
A_1 & \ldots & a_{10} & a_{11} & a_{12} & a_{13} & \ldots \\
A_2 & \ldots & a_{20} & a_{21} & a_{22} & a_{23} & \ldots \\
A_3 & \ldots & a_{30} & a_{31} & a_{32} & a_{33} & \ldots \\
 & & \vdots & & & &
\end{array}$$

[1] Preporučamo i sljedeću literaturu o dijagonalnom postupku: I. Mihalj, *Prebrojivost skupa racionalnih brojeva i konstrukcija zmijaste funkcije*, MFL 215 (2004), 185–190, te M. Radić, *Analitički prikaz nekih injektivnih funkcija sa skupa $\mathbb{N} \times \mathbb{N}$ u skup $\mathbb{N}$*, MFL XXXI (1980./81), str. 13

Sada dijagonalno definiramo traženu bijekciju, tj. uređene parove poredamo u niz na sljedeći način:

$$a_{00} \quad a_{01} \quad a_{10} \quad a_{02} \quad a_{11} \quad a_{20} \quad a_{03} \quad a_{12} \quad \dots$$

Navedena bijekcija je ilustrirana na sljedećoj slici.



Korolar 1.22. *Neka je $(A_j : j \in \mathbb{N})$ familija skupova, pri čemu je za svaki $j \in \mathbb{N}$ skup A_j konačan ili prebrojiv. Tada je skup $\bigcup_{j\in\mathbb{N}} A_j$ konačan ili prebrojiv.*
(Uočite da za razliku od prošle propozicije dopuštamo da članovi familije nisu nužno u parovima disjunktni, te da mogu biti i konačni.)

Dokaz prethodnog korolara dan je kao rješenje zadatka 4 na strani 30.

Korolar 1.23. *Vrijede sljedeće tvrdnje:*

a) skup cijelih brojeva je prebrojiv;

b) skup racionalnih brojeva $\mathbb{Q}$ je prebrojiv;

c) $\mathbb{N} \times \mathbb{N}$, $\mathbb{N}^3, \dots$ su prebrojivi skupovi.

Dokaz. a) $\mathbb{Z}$=$\{1, 2, 3, \dots\} \cup \{0\} \cup \{-1, -2, -3, \dots\}$;

b) Označimo za svaki $k \in \mathbb{N} \setminus \{0\}$ sa $\mathbb{Q}_k$ skup $\{\frac{1}{k}, \frac{2}{k}, \frac{3}{k}, \dots\}$. Očito je svaki skup $\mathbb{Q}_k$ prebrojiv. Tada je $\bigcup_{k\in\mathbb{N}\setminus\{0\}} \mathbb{Q}_k$ prebrojiva unija prebrojivih skupova, a onda iz korolara 1.22. slijedi da je to prebrojiv skup. Pošto je očito $\mathbb{Q}^+ = \bigcup_{k\in\mathbb{N}\setminus\{0\}} \mathbb{Q}_k$ tada

je taj skup prebrojiv. No, $\mathbb{Q} = \mathbb{Q}^+ \cup \{0\} \cup \mathbb{Q}^-$, tj. skup racionalnih brojeva je unija dva prebrojiva skupa i jednog konačnog skupa.

(Prebrojivost skupa $\mathbb{Q}$ se može dokazati i dijagonalnim postupkom.)

c) Neka je za svaki $k \in \mathbb{N}$ definirano $A_k = \{(m,n) : m+n = k\}$. Očito je svaki skup A_k konačan, te za sve $i \neq j$ vrijedi $A_i \cap A_j = \emptyset$. Pošto je $\mathbb{N} \times \mathbb{N} = \bigcup_{k \in \mathbb{N}} A_k$ tada imamo da je $\mathbb{N} \times \mathbb{N}$ prebrojiva unija konačnih skupova. Dalje indukcijom. Q.E.D.

Sljedeći korolar je vrlo važan za kolegij *Matematička logika*.

Korolar 1.24. *Neka je A prebrojiv skup. Označimo sa A^* skup svih konačnih nizova iz A (odnosno, to je skup svih riječi alfabeta A). Tada je skup A^* prebrojiv.*

Propozicija 1.25. *Svaki beskonačan skup sadrži prebrojiv podskup.*

Dokaz. Neka je X neki beskonačan skup. Iz leme 1.11. znamo da postoji injekcija $f : \mathbb{N} \to X$. Očito je $Rng(f)$ jedan prebrojiv podskup od X. Q.E.D.

Napomena 1.26. *Promotrimo sljedeći "dokaz" prethodne propozicije. Pošto je $X \neq \emptyset$ tada po definiciji postoji neki $x_1 \in X$. Pošto je očito $X \setminus \{x_1\} \neq \emptyset$ tada postoji $x_2 \in X \setminus \{x_1\}$. Pošto je očito $X \setminus \{x_1, x_2\} \neq \emptyset$ tada postoji $x_3 \in X \setminus \{x_1, x_2\}$. Rekurzivno možemo definirati niz (x_n). Očito je da je $x_1, x_2, \ldots$ prebrojiv niz čiji svaki član pripada skupu X, te su članovi niza u parovima različiti. No, do sada navedeni aksiomi teorije ZF nam ne omogućavaju dokaz da je klasa $\{x_1, x_2, \ldots\}$ skup.*

Napomena 1.27. *Aksiom prebrojivog izbora (eng. axiom of countable choice) dobivamo kada u AC zahtijevamo da je familija indeksa I prebrojiva. O važnosti tog aksioma za matematičku analizu možete čitati u knjigama [30] (vidi strane 168–170), [31] (vidi strane 112–114) i [18] (vidi str. 44).*

Zadaci.

1. Dokažite propoziciju 1.17.
   Rješenje. Pretpostavimo da skup $\bigcup_{j\in\mathbb{N}} B_j$ nije konačan. Definiramo rekurzivno familiju $(B'_j : j \in \mathbb{N})$ ovako:

$$B'_0 = B_0$$

$$B'_{n+1} = B_{n+1} \setminus (B'_1 \ \cup \ \ldots \ \cup \ B'_n)$$

   Očito vrijedi $\bigcup_{j\in\mathbb{N}} B_j = \bigcup_{j\in\mathbb{N}} B'_j$. Zatim, za svaki $j \in \mathbb{N}$ skup B'_j je konačan, te ako je $i \neq j$ tada je $B'_i \cap B'_j = \emptyset$. Primjenom propozicije 1.16. slijedi tražena tvrdnja.

2. Dokažite lemu 1.18.
   Rješenje. Neka je $A' = A \setminus B$. Očito je tada $A \cup B = A' \cup B$. Pošto je A konačan, te je $A' \subseteq A$, tada iz korolara 1.8. slijedi da je i A' konačan skup. Neka je $k(A') = k$, te neka je $g : A' \to \mathbb{N}_k$ neka bijekcija. Označimo s h jednu bijekciju između B i $\mathbb{N}$. Definiramo funkciju $f : A' \cup B \to \mathbb{N}$ ovako

$$f(x) = \begin{cases} g(x), & \text{ako je } \ x \in A' \\ \\ h(x) + k + 1, & \text{ako je } \ x \in B \end{cases}$$

   Očito je f bijekcija.

3. Dokažite propoziciju 1.19.
   Rješenje. Za svaki $k \in \{0, 1 \ldots, n-1\}$ označimo s B_k skup svih prirodnih brojeva koji pri dijeljenju s brojem n daju ostatak k. Očito je svaki skup B_k prebrojiv. Zatim, za $i \neq j$ vrijedi $B_i \cap B_j = \emptyset$, te imamo $\bigcup_{k\in\mathbb{N}} B_k = \mathbb{N}$. Neka je sa f_k označena neka bijekcija između A_k i B_k. Definiramo funkciju $f : (A_0 \cup \ldots \cup A_{n-1}) \to \mathbb{N}$ tako da elementu x iz skupa A_k pridružimo $f_k(x)$. Očito je funkcija f bijekcija.

4. Dokažite korolar 1.22.
   Rješenje. Pretpostavimo da skup $\bigcup_{j\in\mathbb{N}} A_j$ nije konačan. Rekurzivno definiramo familiju skupova $(A'_j : j \in \mathbb{N})$ ovako:

$$A'_0 = A_0$$

$$A'_{n+1} = A_{n+1} \setminus (A'_1 \ \cup \ \ldots \ \cup \ A'_n)$$

Očito vrijedi $\bigcup_{j\in\mathbb{N}} A_j = \bigcup_{j\in\mathbb{N}} A'_j$. Zatim, za svaki $j \in \mathbb{N}$ skup A'_j je konačan ili prebrojiv, te za $i \neq j$ vrijedi $A'_i \cap A'_j = \emptyset$.

Označimo sa A uniju svih konačnih skupova A'_j. Iz propozicije 1.16. slijedi da je skup A konačan ili prebrojiv. Zatim, označimo s B uniju svih prebrojivih skupova A'_j. Očito vrijedi $\bigcup_{j\in\mathbb{N}} A_j = A \cup B$. Ako je $B = \emptyset$, tj. ne postoji niti jedan prebrojivi skup A'_j, tada je $A \cup B$ konačan ili prebrojiv, a onda i skup $\bigcup_{j\in\mathbb{N}} A_j$.

Ako postoji samo konačno mnogo skupova A'_j koji su prebrojivi tada primjenom propozicije 1.19. slijedi da je skup B prebrojiv. Ako postoji prebrojivo mnogo skupova A'_j koji su prebrojivi tada primjenom prethodne propozicije 1.20. slijedi da je skup B prebrojiv.

Ako je A konačan skup tada iz leme 1.18. slijedi da je skup $A \cup B$ prebrojiv, a onda i skup $\bigcup_{j\in\mathbb{N}} A_j$.

Ako je A prebrojiv skup tada iz propozicije 1.19. slijedi da je skup $A \cup B$ prebrojiv, a onda je i skup $\bigcup_{j\in\mathbb{N}} A_j$ prebrojiv.

5. Neka je A prebrojiv skup. Označimo sa A^* skup svih konačnih nizova iz A (odnosno, to je skup svih riječi alfabeta A). Dokažite da je skup A^* prebrojiv. Rješenje. Za svaki $k \in \mathbb{N} \setminus \{0\}$ skup A^k je prebrojiv (vidi tvrdnju c) korolara 1.23.). Očito vrijedi $A^* \sim \bigcup_{k\in\mathbb{N}\setminus\{0\}} A^k$.

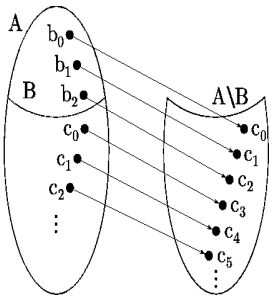
1.4 Neprebrojivi skupovi

Ponovimo definiciju neprebrojivog skupa. Za skup A kažemo da je neprebrojiv ako je beskonačan i nije prebrojiv. Kako bismo mogli navesti neke primjere neprebrojivih skupova moramo prvo dokazati neke činjenice.

Propozicija 1.28. *Neka je A beskonačan i $B \subseteq A$ neki konačan podskup. Tada vrijedi $A \sim A \setminus B$.*

Dokaz. Neka je $B = \{b_0, b_1, \ldots, b_n\}$. Očito je skup $A \setminus B$ beskonačan. Iz propozicije 1.25. slijedi da postoji $C = \{c_0, c_1, c_2, \ldots\}$ prebrojiv podskup od $A \setminus B$.

Na sljedećoj slici je ilustracija ideje dokaza, tj. ideja definicije jedne bijekcije između skupova A i $A \setminus B$.



Sada definiramo funkciju $f : A \to A \setminus B$:

$$f(x) = \begin{cases} c_i, & \text{ako je } x = b_i; \\ c_{n+1+i}, & \text{ako je } x = c_i; \\ x, & \text{ako je } x \in A \setminus (B \cup C). \end{cases}$$

Očito je funkcija f bijekcija. Time smo dokazali $A \sim A \setminus B$. Q.E.D.

Korolar 1.29. *Za sve realne brojeve a i b, takve da je $a < b$, vrijedi:*

$$[a, b] \sim \langle a, b\rangle \sim \langle a, b] \sim [a, b\rangle$$

Korolar 1.30. *Svi omeđeni intervali od $\mathbb{R}$ su međusobno ekvipotentni.*

Dokaz. Prije smo bili dokazali da vrijedi $[a, b] \sim [c, d]$, za sve realne brojeve a, b, c i d, za koje vrijedi $a < b$ i $c < d$. Sada tvrdnja korolara slijedi iz prethodnog korolara 1.29. Q.E.D.

Korolar 1.31. *Svaki omeđeni interval od $\mathbb{R}$ je ekvipotentan sa $\mathbb{R}$.*

Dokaz. Lako je provjeriti da je funkcija

$$f : \mathbb{R} \to \langle -1, 1\rangle \text{ definirana s } f(x) = \frac{x}{1 + |x|}$$

bijekcija. Sada iz korolara 1.30. slijedi tvrdnja. Q.E.D.

Dokazali smo da je skup $\mathbb{R}$ ekvipotentan sa svakim svojim omeđenim intervalom. Sada ćemo prvo dokazati Cantorov teorem o neprebrojivosti skupa $\mathbb{R}$.

Teorem 1.32. *(G. Cantor)*
Skup $\mathbb{R}$ je neprebrojiv.

Dokaz. Očito je dovoljno dokazati da je interval $\langle 0,1\rangle$ neprebrojiv. Pretpostavimo suprotno, tj. da je interval $\langle 0,1\rangle$ prebrojiv. Neka je $\langle 0,1\rangle = \{a_0, a_1, a_2, a_3, \ldots\}$, pri čemu je

$$\begin{aligned} a_0 &= 0.\ a_{00}\ a_{01}\ a_{02}\ \ldots \\ a_1 &= 0.\ a_{10}\ a_{11}\ a_{12}\ \ldots \\ a_2 &= 0.\ a_{20}\ a_{21}\ a_{22}\ \ldots \\ &\vdots \end{aligned}$$

Pretpostavljamo da je svaki realan broj a_i dan u decimalnom zapisu koji ima beskonačno mnogo decimala različitih od nule. Primjerice umjesto 0.5 pišemo $0.49999\ldots$ Za svaki $k \in \mathbb{N}$ definiramo

$$b_k = \begin{cases} a_{kk} + 1, & \text{ako je } \ a_{kk} \in \{0,1,2,\ldots,7\}; \\ 1, & \text{ako je } \ a_{kk} \in \{8,9\}. \end{cases}$$

Definiramo $b = 0.\ b_0\ b_1\ b_2\ b_3\ \ldots$ Primijetimo da je $b \neq 0$ i $b \neq 1$ pa je $b \in \langle 0,1\rangle$. Uočimo $b \neq a_k$, $\forall k \in \mathbb{N}$ (razlikuju se na k–tom decimalnom mjestu). Time je dobivena kontradikcija. Q.E.D.

U knjizi [2], na čiji je sadržaj velikim dijelom utjecao veliki mađarski matematičar P. Erdös, jedan od istaknutih dokaza je i Cantorov dokaz neprebrojivosti skupa $\mathbb{R}$.

Napomena 1.33. *U dokazu prethodnog teorema je korišten dijagonalni postupak. Kao još jednu ilustraciju primjene dijagonalnog postupka dokazujemo da* $\mathbb{R}$ *nije ekvipotentan sa* ${}^{\mathbb{R}}\mathbb{R} = \{f|\ f : \mathbb{R} \to \mathbb{R}\}$.

Pretpostavimo suprotno. Neka je $F : \mathbb{R} \to {}^{\mathbb{R}}\mathbb{R}$ *jedna bijekcija. Definiramo funkciju* $f : \mathbb{R} \to \mathbb{R}$ *na sljedeći način:* $f(x) = F(x)(x) + 1$. *Tvrdimo da ne postoji* $x_0 \in \mathbb{R}$ *tako da vrijedi* $F(x_0) = f$, *tj. da funkcija* F *nije surjekcija. Ako je* $F(x_0) = f$, *za neki* $x_0 \in \mathbb{R}$, *tada imamo da je* $F(x_0)(y) = f(y)$, *za svaki* $y \in \mathbb{R}$. *Posebno vrijedi za* $y = x_0$, *tj. imamo* $F(x_0)(x_0) = f(x_0)$. *U drugu ruku iz definicije funkcije* f *slijedi* $f(x_0) = F(x_0)(x_0) + 1$. *Time smo dobili da vrijedi* $F(x_0)(x_0) = F(x_0)(x_0) + 1$, *čime je dobivena kontradikcija.*

Propozicija 1.34. *Neka je* A *neprebrojiv skup i* $B \subseteq A$ *konačan ili prebrojiv. Tada je* $A \sim A \setminus B$.

Dokaz. Ovaj dokaz je sasvim analogan dokazu propozicije 1.28. Pošto je $B \subseteq A$ tada vrijedi $A = (A \setminus B) \cup B$. Iz toga slijedi da je skup $A \setminus B$ neprebrojiv (inače bi imali da je A unija dva prebrojiva skupa, ili pak unija konačnog i prebrojivog skupa, pa je skup A prebrojiv, što je suprotno pretpostavci propozicije). Posebno imamo da je skup $A \setminus B$ beskonačan.

Iz propozicije 1.25. slijedi da postoji $C \subseteq A \setminus B$ koji je prebrojiv. Neka je $C = \{c_0, c_1, c_2, \ldots\}$. Radi određenosti promatramo slučaj kada je $B = \{b_0, b_1, b_2, \ldots\}$ prebrojiv skup. Sada definiramo funkciju $f : A \to A \setminus B$ ovako:

$$f(x) = \begin{cases} c_{2i}, & \text{ako je } x = b_i; \\ c_{2i+1}, & \text{ako je } x = c_i; \\ x, & \text{ako je } x \in A \setminus (B \cup C). \end{cases}$$

Očito je funkcija f bijekcija, pa imamo $A \sim A \setminus B$. Na sličan način bi dokazali tvrdnju propozicije kada je B konačan skup. Q.E.D.

Primjer 1.35. *1. Vrijedi $\mathbb{R} \setminus \mathbb{Q} \sim \mathbb{R}$, tj. skup svih iracionalnih brojeva je ekvipotentan sa skupom $\mathbb{R}$. Dakle, skup svih iracionalnih brojeva je neprebrojiv.*

2. Označimo sa $\mathcal{A}$ skup svih realnih algebarskih brojeva. Nije teško dokazati da je skup $\mathcal{A}$ prebrojiv. Iz prethodne propozicije slijedi $\mathbb{R} \setminus \mathcal{A} \sim \mathbb{R}$. To znači da je posebno $\mathbb{R} \setminus \mathcal{A} \neq \emptyset$. Time smo dokazali egzistenciju transcendentnih brojeva.[2]

Korolar 1.36. *Ako je A beskonačan, a B konačan ili prebrojiv tada vrijedi $A \cup B \sim A$.*

Dokaz. Pretpostavimo da je $A \cap B = \emptyset$. Ako je skup A prebrojiv tada znamo da je to i $A \cup B$, tj. vrijedi $A \cup B \sim A$. Ako je A neprebrojiv onda iz prethodne propozicije slijedi $A \cup B \sim (A \cup B) \setminus B = A$.
Ako je $A \cap B \neq \emptyset$ tada definiramo $B' = B \setminus A$. Tada imamo da je B' konačan ili prebrojiv skup, te vrijedi $A \cup B = A \cup B'$ i $A \cap B' = \emptyset$. Iz prethodnog dijela dokaza znamo da tada vrijedi $A \cup B' \sim A$. Zbog jednakosti $A \cup B = A \cup B'$ tada slijedi $A \cup B \sim A$. Q.E.D.

Često se prilikom dokaza neizomorfnosti određenih struktura koristi neekvipotentnost nosača struktura. To ilustriramo u sljedećem primjeru.

Primjer 1.37. *1. Grupe $(\mathbb{Z}, +)$ i $(\mathbb{R} \setminus \{0\}, \cdot)$ nisu izomorfne, jer skupovi $\mathbb{Z}$ i $\mathbb{R}$ nisu ekvipotentni.*

[2]Daleko teže je navesti jedan transcendentan broj (naravno, i dokazati njegovu transcendentnost). Brojevi π i e su transcendentni, ali je dokaz njihove transcendentnosti dosta kompliciran. Liouvilleov broj je definiran sa:

$$\sum_{n=1}^{\infty} 10^{-n!} = \frac{1}{10^{1!}} + \frac{1}{10^{2!}} + \frac{1}{10^{3!}} + \dots$$

Dokaz transcendentnosti Liouvilleovog broja možete pronaći u: P. Vuković, Liouvilleovi brojevi, MFL 215 (2004), 182–184 i M. Gobo, Algebarski i transcendenti brojevi, MFL 123 (1980), 141–143. O algebarskim i transcendentnim brojevima možete čitati i u: B. Pavković, D. Veljan, Elementarna matematika 1, Tehnička knjiga, Zagreb, 1992.; S. Kurepa, Matematička analiza 2, Tehnička knjiga, Zagreb,; D. Blanuša, Viša matematika, Tehnička knjiga, Zagreb, 1973.; V. Perić, Sedmi Hilbertov problem i transcendentnost brojeva e i π, Matematika (stručno–metodički časopis), 1990, br. 1. Transcendentni brojevi se ne mogu konstruirati samo pomoću ravnala i šestara. Pošto je dokazano da je broj π transcendentan time je riješen starogrčki problem kvadrature kruga.

2. *Polja* $\mathbb{R}$ *i* $\mathbb{Q}(\sqrt{3})$ *nisu izomorfna.*
Sjetimo se da vrijedi $\mathbb{Q}(\sqrt{3}) = \{a + b\sqrt{3} \ : \ a, b \in \mathbb{Q}\}$. *Očito je taj skup ekvipotentan sa* $\mathbb{Q}^2$. *Bili smo dokazali da je skup* $\mathbb{N}^2$ *prebrojiv. Iz toga slijedi da je i skup* $\mathbb{Q}^2$ *također prebrojiv. To znači da je skup* $\mathbb{Q}(\sqrt{3})$ *prebrojiv.*

1.5 Kardinalnost

Još u osnovnoj školi smo učili da svaki prirodni broj ima dvostruku ulogu: određuje koliko čega ima, te koji je po redu. To znači da je svaki prirodan broj kardinalni (glavni) i redni. Cilj nam je definirati beskonačne kardinalne brojeve koji će mjeriti veličinu beskonačnih skupova, te beskonačne redne brojeve koji će mjeriti poredak beskonačnih skupova. Prvo ćemo definirati redne brojeve (ordinale), a zatim kardinalne brojeve. Svaki kardinalni broj je ordinalni, ali ne i obratno.

Tekst koji slijedi u ovoj točki služi kao motivacija za aksiomatsku izgradnju teorije skupova. Odnosno, želi se istaknuti problem definicije kardinalnog broja, te navesti neke osnovne teoreme o kardinalnosti.

Definicija 1.38. *Ako su* A *i* B *ekvipotentni skupovi tada kažemo još da imaju istu* **kardinalnost**, *te pišemo* $k(A) = k(B)$.

Kardinalnost je zapravo sinonim za ekvipotentnost. To znači da u ovom trenutku još nismo definirali pojam kardinalnog broja. Lako je vidjeti da je relacija "biti ekvipotentan" relacija ekvivalencije (na čemu? – na klasi svih skupova?!). Znamo da svaka relacija ekvivalencije definira particiju (vidi propoziciju 1.60.). Iz tog razloga čini se da bi mogli definirati kardinalni broj proizvoljnog skupa A kao klasu ekvivalencije obzirom na relaciju $\sim$, odnosno

$$k(A) \ = \ \{B : \ B \text{ je skup takav da } \ A \sim B\}.$$

Problem je što niti za jedan skup $A \neq \emptyset$ klasa $k(A)$ nije skup, tj. to je prava klasa. Dokažimo tu tvrdnju. Neka je A proizvoljan neprazan skup. Označimo $C = \{B : B$ je skup i $B \sim A\}$. Pretpostavimo da je C skup. Tada iz aksioma partitivnog skupa slijedi da je $\mathcal{P}(C)$ također skup. Za svaki $x \in \mathcal{P}(C)$ označimo $A_x = A \times \{x\}$. Očito za svaki $x \in \mathcal{P}(C)$ vrijedi $A \sim A_x$, pa je $A_x \in C$ za svaki $x \in \mathcal{P}(C)$. Iz toga slijedi da postoji injekcija iz $\mathcal{P}(C)$ u C, što je nemoguće zbog Cantorovog teorema 1.57., kojeg ćemo navesti kasnije.

Kasnije ćemo definirati kardinalni broj proizvoljnog skupa A kao točno određeni skup iz klase svih skupova koji su ekvipotentni sa skupom A. Radi kraćeg zapisivanja uvodimo neke oznake za kardinalnost:

$$k(\emptyset) = 0 \qquad k(\{0, \ldots, n-1\}) = n$$
$$k(\mathbb{N}) = \aleph_0 \qquad k(\mathbb{R}) = c \ \ (\text{"continuum"})$$

Želimo naglasiti da kada primjerice napišemo $k(A) = \aleph_0$ tada to zapravo znači $A \sim \mathbb{N}$.

Pobrojimo što smo do sada dokazali:

a) $\aleph_0 = k(\mathbb{N}) = k(\{-1, -2, -3, \ldots\}) = k(\mathbb{Q}) = k(\mathbb{Z}) = k(\mathbb{N} \times \mathbb{N}) = k(\mathbb{N}^p)$, za svaki $p \in \mathbb{N} \setminus \{0\}$

b) $k(\mathbb{R}) = k([a, b]) = k(\langle a, b\rangle) = c$, za sve $a, b \in \mathbb{R}$, $a < b$

c) $k(\mathbb{R}) \neq k(\mathbb{N})$, tj. $c \neq \aleph_0$

d) $c \neq k(\{f \mid f : \mathbb{R} \to \mathbb{R}\})$

e) $k(\mathbb{R} \setminus \mathbb{N}) = k(\mathbb{R} \setminus \mathbb{Q}) = k(\mathbb{R} \setminus \mathbb{Z}) = c$

Definicija 1.39. *Kažemo da je* **kardinalnost skupa** A **manja od kardinalnosti skupa** B *ako postoji* $B_1 \subseteq B$ *takav da vrijedi* $A \sim B_1$. *Oznaka:* $k(A) \leq k(B)$.
Ako je $k(A) \leq k(B)$, *te još vrijedi* $k(A) \neq k(B)$ *tada kažemo da je* **kardinalnost skupa** A **strogo manja od kardinalnosti skupa** B. *To označavamo sa* $k(A) < k(B)$.

Lako je vidjeti da vrijedi: $k(A) \leq k(B)$ ako i samo ako skup A možemo injektivno preslikati u skup B. Istaknimo sve moguće situacije prilikom uspoređivanja kardinalnosti dvaju skupova A i B:

a) $k(A) < k(B)$

b) $k(B) < k(A)$

c) $k(A) \leq k(B)$ i $k(B) \leq k(A)$

d) ne vrijedi $k(A) \leq k(B)$ i ne vrijedi $k(B) \leq k(A)$

Dokazat ćemo da su moguća samo prva tri slučaja. Istaknimo sada samo da je nemogućnost slučaja d) ekvivalentna s aksiomom izbora.

Sljedeći teorem je vrlo važan u teoriji skupova. Cantor je prvi iskazao tvrdnju teorema, a njegov devetnaestgodišnji student F. Bernstein ga je 1897. godine prvi dokazao. Poslije ga je više matematičara dokazalo na razne načine. U Velikoj Britaniji se taj teorem naziva Schröder, Bernsteinov teorem, jer ga je 1898. dokazao i Schröder. U Francuskoj i Italiji se naziva Cantor, Bernsteinov teorem.

Teorem 1.40. *(Cantor, Schröder, Bernsteinov teorem)*
Ako postoji injekcija $f : A \to B$ *i injekcija* $g : B \to A$ *tada postoji bijekcija između* A *i* B.

U terminima kardinalnosti teorem se kratko može izreći i na sljedeći način:

Ako je $k(A) \leq k(B)$ *i* $k(B) \leq k(A)$ *tada je* $k(A) = k(B)$.

Prije dokaza prethodnog teorema navodimo Knaster, Tarskijev teorem i Banachovu lemu.

Teorem 1.41. *(Knaster, Tarskijev teorem o fiksnoj točki)*
Neka je $F : \mathcal{P}(A) \to \mathcal{P}(A)$ *monotona funkcija, tj. za sve* $x, y \subseteq A$ *takve da je* $x \subseteq y$ *vrijedi* $F(x) \subseteq F(y)$. *Tada postoji* $x_0 \subseteq A$ *tako da vrijedi* $F(x_0) = x_0$.

Dokaz. Lako je vidjeti da skup $x_0 := \cup\{x \subseteq A \ : \ x \subseteq F(x)\}$ zadovoljava traženi uvjet. Q.E.D.

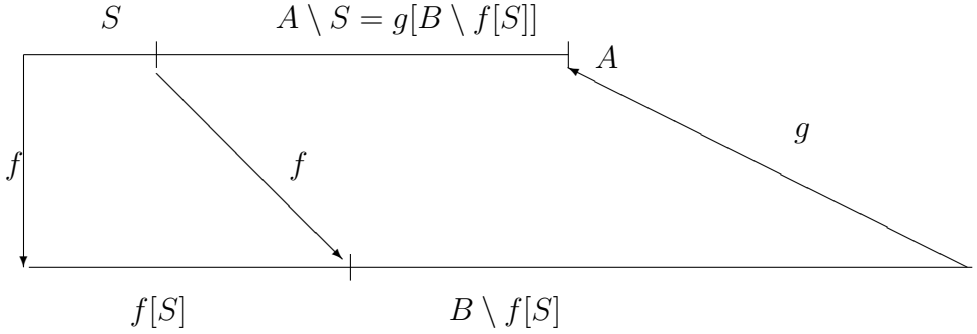
Na strani 45 navest ćemo i detaljno dokazati općenitiji teorem o fiksnoj točki.

Lema 1.42. *(Banachova lema)*
Neka su $f : A \to B$ *i* $g : B \to A$ *proizvoljne funkcije. Tada postoji* $S \subseteq A$ *tako da vrijedi*

$$g[B \setminus f[S]] = A \setminus S.$$

Dokaz. Definiramo funkciju $F : \mathcal{P}(A) \to \mathcal{P}(A)$ ovako: $F(x) = A \setminus (g[B \setminus f[x]])$. Dokažimo da je F monotona funkcija. Neka su x i y podskupovi od A tako da vrijedi $x \subseteq y$. Tada je $f[x] \subseteq f[y]$, a onda je $B \setminus f[y] \subseteq B \setminus f[x]$. Iz toga slijedi $g[[B \setminus f[y]] \subseteq g[B \setminus f[x]]$, a onda $(g[B \setminus f[x]])^c \subseteq (g[B \setminus f[y]])^c$, tj. $F(x) \subseteq F(y)$. Primjenom Knaster, Tarskijevog teorema slijedi tražena tvrdnja leme. Q.E.D.

Dokaz Cantor, Schröder, Bernsteinovog teorema.
Neka su $f : A \to B$ i $g : B \to A$ injekcije. Neka je $S \subseteq A$ koji ima svojstvo iz Banachove leme, tj. $g[B \setminus f[S]] = A \setminus S$. Dana situacija je prikazana na sljedećoj slici.



Pošto je funkcija g injekcija tada je za svaki $x \in A \setminus S$ skup $g^{-1}[\{x\}]$ jednočlan. Za svaki $x \in A \setminus S$ označimo sa b_x element iz $B \setminus f[S]$ za kojeg vrijedi $g^{-1}[\{x\}] = \{b_x\}$.

Definiramo funkciju $h : A \to B$ ovako:

$$h(x) = \begin{cases} f(x)\,, & x \in S \\ b_x\,, & x \in A \setminus S \end{cases}$$

Svojstvo skupa S povlači da je h injekcija, te još vrijedi

$$h[A] = h[S] \cup h[A \setminus S] = f[S] \cup g^{-1}[A \setminus S] = f[S] \cup (B \setminus f[S]) = B.$$

To znači da je funkcija h i surjekcija. Q.E.D.

Primjer 1.43. *U ovom primjeru ilustrirat ćemo primjenu Cantor, Schröder, Bernsteinovog teorema prilikom dokaza da su skupovi $\mathbb{R}^2$ i $\mathbb{R}$ ekvipotentni. Dovoljno je vidjeti da postoji injekcija sa skupa $\mathbb{R}^2$ u $\mathbb{R}$, i obratno. Jedna injekcija iz $\mathbb{R}$ u $\mathbb{R}^2$ je dana s $x \mapsto (x, 0)$. Pošto je $\mathbb{R} \sim \langle 0, 1\rangle$, tada je očito $\langle 0, 1\rangle \times \langle 0, 1\rangle \sim \mathbb{R} \times \mathbb{R}$. Iz tog razloga je umjesto injekcije iz $\mathbb{R}^2$ u $\mathbb{R}$ dovoljno navesti jednu injekciju iz $\langle 0, 1\rangle \times \langle 0, 1\rangle$ u $\mathbb{R}$. Jedna injekcija iz $\langle 0, 1\rangle \times \langle 0, 1\rangle$ u $\mathbb{R}$ dana je s*

$$(0.a_0a_1\ldots\ ,\ 0.b_0b_1\ldots) \mapsto 0.a_0\ 1\ b_0\ 1\ a_1\ 1\ b_1\ldots$$

Sada ćemo razmatrati operacije vezane s kardinalnošću.

Definicija 1.44. *Neka su A i B skupovi. Neka je $A' = A \times \{0\}$ i $B' = B \times \{1\}$. Očito su skupovi A' i B' disjunktni, te vrijedi $k(A) = k(A')$ i $k(B) = k(B')$. Tada sa $k(A) + k(B)$ označavamo $k(A' \cup B')$.*

Propozicija 1.45. *Neka su A, B i C skupovi, te a, b i c redom oznake za njihove kardinalnosti. Tada vrijedi:*

1) $a + b = b + a$

2) $(a + b) + c = a + (b + c)$

3) $a + 0 = a$

4) ako je $a \leq b$ *tada je* $a + c \leq b + c$

Dokaz tvrdnje a). Neka su A i B skupovi za koje vrijedi $k(A) = a$ i $k(B) = b$. Pošto je očito $A' \cup B' \sim B' \cup A'$ tada imamo:

$$a + b = k(A) + k(B) = k(A' \cup B') = k(B' \cup A') = k(B) + k(A) = b + a.$$ Q.E.D.

Napomena 1.46. *Općenito ne vrijedi da $a + b = a + c$ povlači $b = c$. Primjerice vrijedi $\aleph_0 + 1 = \aleph_0 + 2$, ali $1 \neq 2$.*

Primjer 1.47. *Lako je vidjeti da vrijedi:*

$$2 + 2 = 4 \qquad \aleph_0 + \aleph_0 = \aleph_0 \qquad c + \aleph_0 = c \qquad c + c = c$$

Sljedeći korolar je jednostavna posljedica propozicije 1.34.

Korolar 1.48. *Neka je A proizvoljan beskonačan skup. Tada za svaki $n \in \mathbb{N}$ vrijedi $k(A) + n = k(A)$, te vrijedi $k(A) + \aleph_0 = k(A)$.*

Definicija 1.49. *Neka su A i B proizvoljni skupovi. Tada s $k(A) \cdot k(B)$ označavamo $k(A \times B)$.*

Propozicija 1.50. *Neka su A, B i C skupovi, te a, b i c redom oznake za njihove kardinalnosti. Tada vrijedi:*

1) $a \cdot b = b \cdot a$

2) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

3) $a \cdot 1 = a$

4) ako je $a \leq b$ *tada je* $a \cdot c \leq b \cdot c$

Napomena 1.51. *Općenito ne vrijedi da $a \cdot b = a \cdot c$ povlači $b = c$. Primjerice vrijedi $\aleph_0 \cdot 2 = \aleph_0 \cdot 3$, ali $2 \neq 3$.*

Primjer 1.52. *Lako je vidjeti da vrijedi:*

$$2 \cdot 2 = 4 \qquad \aleph_0 \cdot \aleph_0 = \aleph_0 \qquad c \cdot \aleph_0 = c \qquad c \cdot c = c$$

Zašto je rezultat $c \cdot c = c$, tj. $k(\mathbb{R}^2) = k(\mathbb{R})$, pomalo neočekivan? Zato što se protivi našoj intuiciji dimenzije. No, to zapravo samo znači da dimenzije nisu sačuvane kod bijektivnih preslikavanja. Brouwer je dokazao da neprekidne bijekcije, čiji inverz je također neprekidan, čuvaju dimenziju.

Na kraju, kada ćemo govoriti o aksiomu izbora, dokazat ćemo da za sve kardinalnosti $a \neq 0$ i $b \neq 0$, od kojih je bar jedna beskonačna, vrijedi

$$a + b = a \cdot b = \max\{a, b\}$$

Definicija 1.53. *Neka su A i B skupovi. Označimo ${}^AB = \{f | f : A \to B\}$. Tada sa $k(B)^{k(A)}$ označavamo $k({}^AB)$.*

Namjera nam je da oznaka za skup svih funkcija iz A u B, odnosno ${}^AB$, bude sugestivna. U drugu ruku, želimo primjerice da 3^2 bude i dalje jednako 9. Koristeći upravo uvedene definicije za ilustraciju izračunajmo 3^2. Neka je A neki dvočlani skup, a B neki tročlani skup. Tada po definiciji imamo: $3^2 = k(B)^{k(A)} = k({}^AB) = k(\{f | f : A \to B\}) = 9$.

Propozicija 1.54. *Za svaki skup A vrijedi $\mathcal{P}(A) \sim {}^A\{0, 1\}$, tj. $k(\mathcal{P}(A)) = 2^{k(A)}$.*

Dokaz. Funkcija $A \supseteq B \mapsto \chi_B : A \to \{0, 1\}$ je očito bijekcija. (Sa χ_B je označena karakteristična funkcija skupa B). Q.E.D.

Propozicija 1.55. *Neka su A, B i C skupovi, te a, b i c redom oznake za njihove kardinalnosti. Tada vrijedi:*

1) $a^b \cdot a^c = a^{b+c}$

2) $(a^b)^c = a^{b \cdot c}$

3) $(a \cdot b)^c = a^c \cdot b^c$

4) ako je $a \leq b$ *tada je* $a^c \leq b^c$

5) ako je $a \leq b$ *i* $c \neq 0$ *tada je* $c^a \leq c^b$

Primjer 1.56. *Kako bi dokazali da vrijedi $2^{\aleph_0} = c$ dokazujemo da je ${}^{\mathbb{N}}\{0,1\} \sim \mathbb{R}$. U tu svrhu primijetimo da su sljedeće dvije funkcije injekcije: ${}^{\mathbb{N}}\{0,1\} \ni (x_n) \mapsto 0.x_0x_1x_2\ldots \in \mathbb{R}$; $\langle 0,1\rangle \ni 0.x_0x_1x_2\ldots \mapsto (x_n) \in {}^{\mathbb{N}}\{0,1\}$ (svaki element iz intervala $\langle 0,1\rangle$ promatramo u decimalnom prikazu s beskonačno mnogo decimala različitih od nule). Sada primijenimo Cantor, Schröder, Bernsteinov teorem, pa imamo $2^{\aleph_0} = c$.*

Koristeći prethodni rezultat dokažimo sada da vrijedi $c^{\aleph_0} = c$:

$$c^{\aleph_0} = (2^{\aleph_0})^{\aleph_0} = 2^{\aleph_0 \cdot \aleph_0} = 2^{\aleph_0} = c.$$

Sada dokazujemo da vrijedi ${\aleph_0}^{\aleph_0} = c$. Očito vrijede sljedeće nejednakosti: $\aleph_0^{\aleph_0} \leq c^{\aleph_0} = c$ i $c = 2^{\aleph_0} \leq {\aleph_0}^{\aleph_0}$. Sada primijenimo Cantor, Schröder, Bernsteinov teorem, pa dobivamo ${\aleph_0}^{\aleph_0} = c$.

Teorem 1.57. *(Osnovni Cantorov teorem teorije skupova)*
Za svaki skup A vrijedi $k(A) < k(\mathcal{P}(A))$, tj. $k(A) < 2^{k(A)}$.

Dokaz. Iz definicije relacije $<$ slijedi da treba dokazati: $k(A) \leq k(\mathcal{P}(A))$ i $k(A) \neq k(\mathcal{P}(A))$.
Ako je $A = \emptyset$ tada je $\mathcal{P}(\emptyset) = \{\emptyset\}$. To znači da je u ovom slučaju $k(A) < k(\mathcal{P}(A))$.
Neka je sada $A \neq \emptyset$. Primijetimo prvo da je $k(A) \leq k(\mathcal{P}(A))$, jer je funkcija $f : A \to \mathcal{P}(A)$, koja je definirana sa $f(x) = \{x\}$, injekcija.
Dokažimo sada još $k(A) \neq k(\mathcal{P}(A))$. Pretpostavimo suprotno tj. da je $k(A) = k(\mathcal{P}(A))$, odnosno da vrijedi $A \sim \mathcal{P}(A)$. Neka je $f : A \to \mathcal{P}(A)$ neka bijekcija. Definiramo skup $B = \{x \in A \mid x \notin f(x)\}$. Primijetimo da je $B \neq \emptyset$, jer je $f : A \to \mathcal{P}(A)$ bijekcija pa i surjekcija, a budući da je $\emptyset \in \mathcal{P}(A)$ tada postoji $x \in A$ takav da $f(x) = \emptyset$. No, onda za taj x vrijedi $x \notin f(x)$ tj. $x \in B$.
Neka je $b \in A$ takav da vrijedi $f(b) = B$. Ako bi vrijedilo $b \in B$, tada iz $B = f(b)$ i definicije skupa B slijedi $b \notin f(b)$. Dakle, mora biti $b \notin B = f(b)$. Tada iz definicije skupa B slijedi $b \in B$. Time je dobivena kontradikcija. To znači da ne postoji bijekcija između A i $\mathcal{P}(A)$. Q.E.D.

Napomena 1.58. *Neprebrojivost skupa realnih brojeva možemo dobiti kao jednostavnu posljedicu prethodnog teorema. Iz primjera 1.56. znamo da vrijedi $\mathbb{R} \sim {}^{\mathbb{N}}\{0,1\}$. Iz propozicije 1.54. znamo $\mathcal{P}(\mathbb{N}) \sim {}^{\mathbb{N}}\{0,1\}$. Iz Osnovnog Cantorovog teorema znamo $\mathcal{P}(\mathbb{N}) \not\sim \mathbb{N}$. Iz svega toga slijedi $\mathbb{R} \not\sim \mathbb{N}$.*

Cantorova hipoteza kontinuuma

Zašto uopće teoriju skupova promatrati aksiomatski? Već smo bili naglasili da je glavno pitanje ovog kolegija: "Što je skup?" Odgovor na to pitanje pokušat ćemo dati uvođenjem aksiomatskog sistema. Drugi razlog nezadovoljstva s naivnom (neaksiomatskom) teorijom skupova je svakako pojava paradoksa. O tome smo već bili prije govorili. Sljedeći razlog aksiomatskog zasnivanja bio je nemogućnost odgovora na neka pitanja o skupovima koja su se prirodno nametala. Možda jedno od najpoznatijih pitanja, i jedno od razumljivih na ovom samom početku priče o teoriji ZF, je svakako *Cantorova hipoteza kontinuuma*. To je sljedeća tvrdnja:

> *ako je S beskonačan podskup skupa $\mathbb{R}$ tada postoji bijekcija sa S na $\mathbb{N}$ ili sa S na $\mathbb{R}$.*

Dugo se pokušavala dokazati, a i opovrgnuti ta hipoteza. No, svi pokušaji u naivnoj teoriji skupova su bili bezuspješni. P. Cohen je 1963. godine dokazao da je Cantorova hipoteza kontinuuma **neodlučiva** u teoriji ZF. To znači da je u danoj teoriji ne možemo dokazati, a ni opovrgnuti. O Cohenovom dokazu možete čitati u [11], [18] i [21].

Paul Cohen, 1934.–2007.

Zadaci

1. Neka su A i B proizvoljni skupovi. Dokažite da vrijedi $k(A) \leq k(B)$ ako i samo ako skup A možemo injektivno preslikati u skup B.
2. Dokažite Knaster, Tarskijev teorem o fiksnoj točki.
3. Dokažite propoziciju 1.45.
4. Dokažite da vrijedi: $\aleph_0 + \aleph_0 = \aleph_0$, $c + \aleph_0 = c$ i $c + c = c$.
5. Dokažite propoziciju 1.50.
6. Dokažite da vrijedi: $\aleph_0 \cdot \aleph_0 = \aleph_0$, $c \cdot \aleph_0 = c$ i $c \cdot c = c$.
7. Dokažite propoziciju 1.55.

1.6 Uređeni skupovi

Neka je A neki skup. Svaki podskup R od $A \times A$ nazivamo **binarna relacija**. Činjenicu $(x, y) \in R$ zapisujemo i xRy.

Kažemo da je binarna relacija R:

a) **refleksivna**, ako za svaki $x \in A$ vrijedi xRx

b) **irefleksivna**, ako ne postoji $x \in A$ tako da vrijedi xRx

c) **simetrična**, ako za sve $x, y \in A$ koji imaju svojstvo xRy vrijedi yRx

d) **antisimetrična**, ako za sve $x, y \in A$ koji imaju svojstvo xRy i yRx vrijedi $x = y$

e) **tranzitivna**, ako za sve $x, y, z \in A$ koji imaju svojstvo xRy i yRz vrijedi xRz

f) **relacija ekvivalencije**, ako je refleksivna, simetrična i tranzitivna;
za $x \in A$ skup $\{y \in A : xRy\}$ nazivamo klasa ekvivalencije, i označavamo ga s $[x]$.

Kako bismo mogli izreći sljedeću propoziciju prvo ćemo dati definiciju particije skupa.

Definicija 1.59. *Neka je $A \neq \emptyset$ proizvoljan skup. Kažemo da je familija skupova $\mathcal{F}$* **particija skupa** *A ako vrijedi:*

a) za svaki $x \in \mathcal{F}$ je $x \subseteq A$;

b) za svaki $x \in \mathcal{F}$ je $x \neq \emptyset$;

c) za sve $x, y \in \mathcal{F}$, $x \neq y$, vrijedi $x \cap y = \emptyset$;

d) $\bigcup_{x \in \mathcal{F}} x = A$.

Propozicija 1.60. *Svaka relacija ekvivalencije definira jednu particiju skupa, i obratno.*

U daljnjim izlaganjima razmatrat ćemo uređene skupove. Sjetimo se: želimo definirati pojam "nivoa" (točnije: ordinalnog broja) kako bismo definirali kumulativnu hijerarhiju.

Definicija 1.61. *Neka je R binarna relacija na skupu A. Kažemo da je R relacija* **parcijalnog uređaja** *ako je irefleksivna i tranzitivna. Relaciju parcijalnog uređaja obično označavamo sugestivno $s <$ ili $\prec$. Uređeni par $(A, <)$ nazivamo* **parcijalno uređen skup**.

Ako je $(A, <)$ parcijalno uređen skup tada možemo definirati binarnu relaciju $\leq$ sa:

$$x \leq y \qquad \text{ako i samo ako} \qquad x < y \ \text{ ili } \ x = y.$$

Očito je relacija $\leq$ refleksivna, antisimetrična i tranzitivna. Relacije $<$ i $\leq$ su međusobno definabilne.

Primjer 1.62. *Primjeri parcijalno uređenih skupova.*

a) Prirodni ili standardni uređaj na skupovima $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ *i* $\mathbb{R}$ *definiran je sa:*

$$x < y \qquad \textit{ako i samo ako} \qquad (\exists z > 0)(x + z = y)$$

Očito su skupovi $(\mathbb{N}, <)$, $(\mathbb{Z}, <)$, $(\mathbb{Q}, <)$ *i* $(\mathbb{R}, <)$ *parcijalno uređeni skupovi.*

b) **Leksikografski** *uređaj na skupu* $\mathbb{N} \times \mathbb{N}$ *definiran je sa:*

$$(x_1, y_1) \prec (x_2, y_2) \quad \textit{ako i samo ako} \quad (x_1 < x_2) \ \textit{ ili } \ (x_1 = x_2 \ \textit{ i } \ y_1 < y_2)$$

Lako je provjeriti da je skup $(\mathbb{N} \times \mathbb{N}, \prec)$ *parcijalno uređen skup.*

c) **Antileksikografski** *uređaj na skupu* $\mathbb{N} \times \mathbb{N}$ *definiran je sa:*

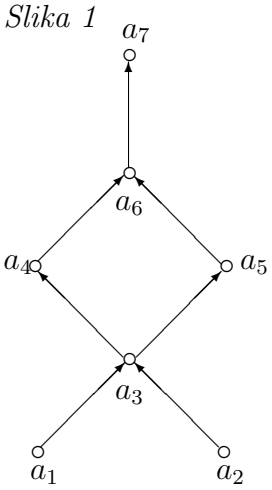
$$(x_1, y_1) \prec (x_2, y_2) \quad \textit{ako i samo ako} \quad (y_1 < y_2) \ \textit{ ili } \ (y_1 = y_2 \ \textit{ i } \ x_1 < x_2)$$

Lako je provjeriti da je skup $(\mathbb{N} \times \mathbb{N}, \prec)$ *parcijalno uređen skup.*

d) Ako je A *skup tada je* $(\mathcal{P}(A), \subset)$ *parcijalno uređen skup.*

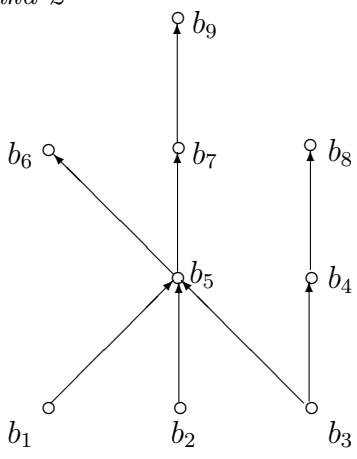
e) Sada navodimo dva primjera parcijalno uređenih skupova koji su definirani pomoću grafa (tj. pomoću tzv. Hasseovih dijagrama). Strelice označavaju uređaj. Primjerice, na Slici 1 strelica između a_4 *i* a_6 *označava da vrijedi* $a_4 < a_6$*. Važno je još naglasiti da ne pretpostavljamo da je relacija uređaja tranzitivna. To ćemo posebno naglasiti kada podrazumijevamo tranzitivnost, ali na slikama to nećemo posebno isticati.*

Slika 1



$A = \{a_1, \ldots, a_7\}$

Slika 2



$B = \{b_1, \ldots, b_9\}$

Definicija 1.63. *Neka je $(A, <)$ parcijalno uređen skup. Kažemo da:*

a) elementi x i y su **usporedivi** *ako vrijedi $x \leq y$ ili $y \leq x$; inače kažemo da su elementi x i y* **neusporedivi***;*

b) skup $B \subseteq A$ je **lanac** *ako su svi elementi skupa B usporedivi;*

c) element $x \in A$ je **maksimalan** *(***minimalan***) ako ne postoji $y \in A$ tako da vrijedi $x < y$ $(y < x)$;*

d) element $x \in A$ je **najveći** *(***najmanji***) ako za svaki $y \in A$ vrijedi $y \leq x$ $(x \leq y)$;*

Najveći je onaj element koji je veći od svih ostalih. Maksimalni je onaj element od kojeg ne postoji veći. Na *Slici 1* u skupu A imamo dva minimalna elementa, te postoji najveći element, ako pretpostavljamo da je relacija uređaja tranzitivna. Na *Slici 2* u skupu B postoje tri minimalna elementa i tri maksimalna elementa.

Napomena 1.64. *Neka je $(A, <)$ neki parcijalno uređen skup. Tada vrijedi:*

a) ako je $x \in A$ najveći (najmanji) element tada je x i maksimalni (minimalni) element u skupu A.

b) ako u skupu A ne postoji niti jedan maksimalni (minimalni) element tada A nema ni najveći (najmanji) element;

c) ako u skupu A postoji više od jednog maksimalnog (minimalnog) elementa tada A nema najveći (najmanji) element;

d) ako je $x \in A$ jedinstveni maksimalni (minimalni) element u skupu A tada x ne mora biti najveći (najmanji) element skupa A. Za ilustraciju ove napomene navodimo sljedeći primjer. Neka je $A = \mathbb{N} \cup \{\frac{1}{2}\}$. Na skupu $\mathbb{N}$ promatramo standardni uređaj, te definiramo da broj $\frac{1}{2}$ nije usporediv niti s jednim prirodnim brojem. Tada je $\frac{1}{2}$ jedinstveni maksimalni element, ali nije najveći element u skupu A.

Definicija 1.65. *Neka je $(A, <)$ parcijalno uređen skup, te $\emptyset \neq B \subseteq A$.*

a) Za element x od A kažemo da je **gornja (donja) međa** *skupa B ako za svaki $y \in B$ vrijedi $y \leq x$ $(x \leq y)$;*

b) Za $B \subseteq A$ kažemo da je **omeđen odozgo (odozdo)** *ako za B postoji gornja (donja) međa. Ako je skup B omeđen odozgo i odozdo tada kažemo da je* **omeđen**.

c) Za element x od A kažemo da je **supremum (infimum)** *skupa B ako je x najmanja gornja (najveća donja) međa skupa B.*

Ako je $x \in A$ tada skup $p_A(x) = \{y \in A : y < x\}$ nazivamo **početni komad** *elementa x u skupu A.*

Sljedeću propoziciju je lako dokazati indukcijom (vidi zadatak 6 na strani 47).

Propozicija 1.66. *Neka je $(A, <)$ konačan parcijalno uređen skup. Tada skup A sadrži maksimalan i minimalan element.*

Definicija 1.67. *Za parcijalno uređen skup kažemo da je* **linearno uređen** *(potpuno ili totalno) ako su svaka dva njegova različita elementa usporediva.*

Skupovi $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ i $\mathbb{R}$ sa standardnim uređajem su linearno uređeni.

Definicija 1.68. *Neka su $(A, <)$ i $(B, \prec)$ parcijalno uređeni skupovi. Kažemo da funkcija $f : A \to B$* **čuva uređaj** *ako vrijedi:*

$$(\forall x, y \in A)(x \leq y \Rightarrow f(x) \preceq f(y))$$

Teorem 1.69. *(Teorem o fiksnoj točki)*
Neka je $(A, <)$ parcijalno uređen skup koji ima najmanji (najveći) element, te neka je $f : A \to A$ funkcija koja čuva uređaj. Tada vrijedi:

> *ako za svaki $\emptyset \neq B \subseteq A$ postoji supremum (infimum) tada postoji najveća (najmanja) fiksna točka za funkciju f.*

Dokaz. Pretpostavimo da za svaki neprazan podskup od B postoji supremum u skupu A. Neka je $B = \{x \in A : x \leq f(x)\}$. Ako je $a \in A$ najmanji element tada očito vrijedi $a \in B$, tj. $B \neq \emptyset$. Neka je $b = \sup B$. Za svaki $x \in B$ vrijedi $x \leq b$. Pošto f čuva uređaj tada imamo $f(x) \leq f(b)$. Sada zbog $x \leq f(x)$ (definicija skupa B), te tranzitivnosti, dobivamo da za svaki $x \in B$ vrijedi $x \leq f(b)$. Iz toga slijedi da je $f(b)$ jedna gornja međa skupa B. Pošto je $b = \sup B$, tada imamo

$$b \leq f(b) \qquad (*)$$

Dokažimo sada drugu nejednakost. Iz $(*)$ slijedi $f(b) \leq f(f(b))$, a onda je $f(b) \in B$. Pošto je $b = \sup B$, tada je $f(b) \leq b$.

Preostalo je dokazati da je b najveća fiksna točka. Neka je $a \in A$ tako da vrijedi $f(a) = a$. Posebno tada vrijedi $a \leq f(a)$, pa je $a \in B$. Pošto je $b = \sup B$, tada imamo $a \leq b$.
(Za najmanju fiksnu točku treba promatrati skup $\{x \in A : f(x) \leq x\}$). Q.E.D.

Sljedeći korolar bili smo već dokazali (vidi teorem 1.41.) No, ovdje ga ipak ističemo jer je jednostavna posljedica prethodnog teorema.

Korolar 1.70. *(Knaster, Tarskijev teorem)*
Neka je A neprazan skup i $F : \mathcal{P}(A) \to \mathcal{P}(A)$ funkcija takva da za sve $x, y \subseteq A$ vrijedi da $x \subseteq y$ povlači $F(x) \subseteq F(y)$. Tada postoji $x_0 \subseteq A$ tako da vrijedi $F(x_0) = x_0$.

Napomena 1.71. *Primjenom prethodnog korolara bili smo dokazali egzistenciju skupa S koji treba za dokaz Cantor, Schröder, Bernsteinovog teorema. Obično se u Knaster, Tarskijev teoremu navodi da za:*

$$fix(F) = \bigcap\{x : x \subseteq A,\ F(x) \subseteq x\},$$
$$Fix(F) = \bigcup\{x : x \subseteq A,\ x \subseteq F(x)\},$$

vrijedi da je $fix(F)$ najmanja, a $Fix(F)$ najveća fiksna točka funkcije f. Primijetite da je skup $Fix(F)$ upravo definiran kao supremum skupa $\{x : x \subseteq A,\ x \subseteq F(x)\}$, tj. upravo kao i fiksna točka iz dokaza prethodnog teorema o fiksnoj točki.

Definicija 1.72. *Neka su $(A, <)$ i $(B, \prec)$ parcijalno uređeni skupovi. Svaku bijekciju $f : A \to B$ koja ima svojstvo da f i f^{-1} čuvaju uređaj nazivamo* **sličnost** *(ili izomorfizam). Kažemo da su parcijalno uređeni skupovi A i B* **slični skupovi** *ako postoji barem jedna sličnost $f : A \to B$. Ako su A i B slični skupovi tada to označavamo sa $A \simeq B$.*

Primjer 1.73.

1. *Vrijedi $\langle 0, 1\rangle \simeq \langle 2, 4\rangle$. Jedna sličnost $f : \langle 2, 4\rangle \to \langle 0, 1\rangle$ je zadana sa $f(x) = \dfrac{x-2}{2}$.*
2. *Očito vrijedi $\mathbb{N} \simeq 2\mathbb{N}$.*
3. *Vrijedi $\mathbb{R} \simeq \langle -\dfrac{\pi}{2}, \dfrac{\pi}{2}\rangle$, jer je restrikcija $tg|_{\langle -\frac{\pi}{2}, \frac{\pi}{2}\rangle} : \langle -\frac{\pi}{2}, \frac{\pi}{2}\rangle \to \mathbb{R}$ sličnost.*

Napomena 1.74. *Ako vrijedi $A \simeq B$ tada očito $A \sim B$. No, obrat općenito ne vrijedi (primjerice $\mathbb{N} \sim \mathbb{Z}$, ali ne i $\mathbb{N} \simeq \mathbb{Z}$).*

Definicija 1.75. *Kažemo da je linearno uređen skup $(A, <)$* **gust** *ako sadrži barem dva elementa, i za sve $x, y \in A$ takve da je $x < y$ postoji $z \in A$ tako da vrijedi $x < z$ i $z < y$.*

Propozicija 1.76. *(Invarijante sličnosti)*
Neka su A i B slični parcijalno uređeni skupovi. Tada vrijedi:

a) skup A je linearno uređen ako i samo ako B je linearno uređen;

b) skup A ima maksimalni (minimalni) element ako i samo ako B sadrži maksimalni (minimalni) element;

c) skup A ima najveći (najmanji) element ako i samo ako skup B ima najveći (najmanji) element;

d) skupa A je gust ako i samo ako skup B je gust.

Primijetite da iz prethodne propozicije primjerice slijedi $\mathbb{N} \not\simeq \mathbb{Z}$ i $\mathbb{Q} \not\simeq \mathbb{Z}$.

Zadaci

1. Neka je R relacija ekvivalencije na skupu A. Dokažite da tada za sve $x, y \in A$ vrijedi: $[x] = [y]$ ili $[x] \cap [y] = \emptyset$.

2. Dokažite propoziciju 1.60.

3. Neka je $\sim$ binarna relacija na $\mathbb{N} \times \mathbb{N}$ definirana s $(x_1, y_1) \sim (x_2, y_2)$ ako vrijedi $x_1 + y_2 = y_1 + x_2$. Dokažite da je $\sim$ relacija ekvivalencije.

4. Neka je $\sim$ binarna relacija na $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ definirana sa: $(x_1, y_1) \sim (x_2, y_2)$ ako vrijedi $x_1 \cdot y_2 = y_1 \cdot x_2$. Dokažite da je $\sim$ relacija ekvivalencije.

5. Označimo s A skup svih Cauchyevih nizova racionalnih brojeva. Na skupu A definiramo binarnu relaciju $\sim$ ovako:

$$(a_n) \sim (b_n) \text{ ako i samo ako } \lim_{n\to\infty} (a_n - b_n) = 0.$$

   Dokažite da je $\sim$ relacija ekvivalencije.

6. Dokažite propoziciju 1.66.
   Dokaz. Dokazujemo da postoji maksimalan element. Analogno bi se dokazalo da postoji minimalni element. Dokaz provodimo indukcijom po broju elemenata skupa A. Ako je A jednočlan skup tada je jedini element ujedno i maksimalni. Pretpostavimo da tvrdnja vrijedi za neki $n \in \mathbb{N}$, te neka je A skup koji sadrži $n+1$ element. Neka je $a \in A$ proizvoljan, ali fiksiran. Označimo $B = A \setminus \{a\}$. Iz pretpostavke indukcije slijedi da skup B sadrži barem jedan maksimalni element. Neka je $B' \subseteq B$ skup svih maksimalnih elemenata skupa B. Promatramo dva slučaja:

   a) element a je neusporediv sa svakim elementom iz B'. Tada je svaki element skupa $B' \cup \{a\}$ maksimalni element skupa A.
   b) postoji barem jedan $x \in B'$ tako da su a i x usporedivi.
      Ako vrijedi $x < a$ tada je a jedan maksimalni element skupa A. Ako pak je $a < x$ tada je B' skup svih maksimalnih elemenata skupa A.

7. Neka je $(A, <)$ konačan parcijalno uređen skup. Dokažite da tada svaki neprazni lanac od A sadrži najmanji i najveći element.

8. Neka je $A \neq \emptyset$ i $R \subseteq A \times A$ antisimetrična relacija. Postoji li nužno $R' \subseteq A \times A$ relacija parcijalnog uređaja takva da je $R \subseteq R'$?
   Rješenje. Ne. Npr. uzmemo li $A = \{a, b, c\}$ i $R = \{(a, b),\ (b, c),\ (c, a)\}$. Očito je relacija R antisimetrična. Ako je $R' \subseteq A \times A$ i $R \subseteq R'$ tranzitivna tada je nužno $(a, c),\ (b, a),\ (c, b) \in R'$. No, tada imamo $(a, b),\ (b, a) \in R'$, pa R' nije antisimetrična.

9. Dokažite propoziciju 1.76.

1.7 Uređajne karakterizacije skupova $\mathbb{Q}$ i $\mathbb{R}$

U ovoj točki dokazat ćemo dva važna teorema koji govore o uređajnoj karakterizaciji skupova $\mathbb{Q}$ i $\mathbb{R}$.

Teorem 1.77. *(Uređajna karekterizacija skupa $\mathbb{Q}$)*
Neka je $(A, \prec)$ linearno uređen skup koji ima sljedeća svojstva:

a) skup A je prebrojiv;

b) skup A je gust;

c) ne postoji ni najmanji, a ni najveći element skupa A.

Tada je skup $(A, \prec)$ sličan sa $(\mathbb{Q}, <)$.

Dokaz. Pošto je po pretpostavci skup A prebrojiv tada njegove elemente možemo poredati u niz. Neka je $A = \{a_0, a_1, \ldots\}$ (naravno, ako je $i < j$ tada ne mora biti $a_i \prec a_j$). Analogno je $\mathbb{Q} = \{q_0, q_1, \ldots\}$. Definirat ćemo funkciju $\varphi : A \to \mathbb{Q}$, iz čije će definicije odmah biti jasno da je sličnost. Istovremeno s definiranjem funkcije φ definiramo induktivno niz (e_n) u skupu A. (Vidjet ćemo na kraju da je $\{e_n : n \in \mathbb{N}\} = A$).

Neka je $e_0 := a_0$ i $\varphi(e_0) := q_0$. Pretpostavimo da je za neki $n \in \mathbb{N}\setminus\{0\}$ definirano $e_0, \ldots, e_{n-1}$ i $\varphi(e_0), \ldots, \varphi(e_{n-1})$. Označimo $E = \{e_0, \ldots, e_{n-1}\}$. Prilikom definicije e_n i $\varphi(e_n)$ razlikujemo dva slučaja:

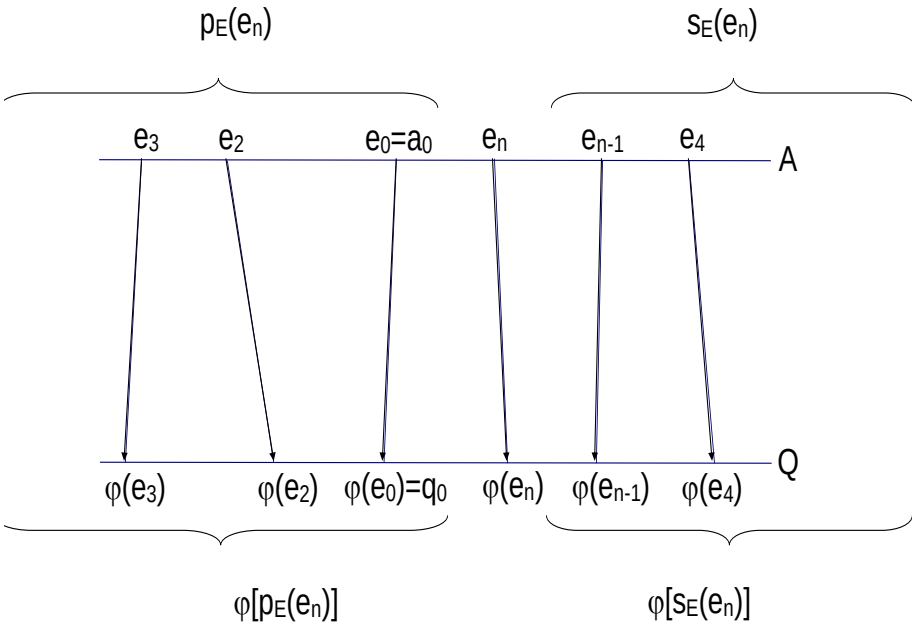
a) n je neparan broj;

b) n je paran broj.

Promatramo prvo slučaj kada je n neparan (tada "iscrpljujemo" skup A.) Neka je

$$j_0 = \min\{k \in \mathbb{N} : a_k \in A \setminus E\},$$

te $e_n = a_{j_0}$. (Dakle, e_n je element iz $A \setminus E$ s najmanjim indeksom). Primijetite da j_0 postoji, jer je A beskonačan, a E je konačan, pa je skup $A \setminus E$ neprazan.
Preostalo je definirati $\varphi(e_n)$. Na sljedećoj slici ilustriramo ideju kako ćemo izabrati element $\varphi(e_n)$.



Neka je

$$p_E(e_n) = \{x \in E : x \prec e_n\} \qquad s_E(e_n) = \{x \in E : e_n \prec x\}$$

(prethodnici u skupu E od elementa e_n) (sljedbenici ...)

Neka je

$$\begin{aligned} k_0 = \min\{k \in \mathbb{N} : \ & q_k \in \mathbb{Q} \setminus \varphi(E), \\ & q_k > x \quad \text{za svaki} \quad x \in \varphi[p_E(e_n)], \\ & q_k < x \quad \text{za svaki} \quad x \in \varphi[s_E(e_n)]\} \end{aligned}$$

Sada definiramo $\varphi(e_n) = q_{k_0}$. (Analogno se tretira slučaj b). Tada "iscrpljujemo" skup $\mathbb{Q}$. Dakle, definiramo prvo $k_0 = \min\{k \in \mathbb{N} : q_k \in \mathbb{Q} \setminus \varphi[E]\}$ i $\varphi(e_n) = q_{k_0}$. Nakon toga definiramo e_n).

Očito je $A = \{e_n : n \in \mathbb{N}\}$. Iz konstrukcije nizova (e_n) i $(\varphi(e_n))$ slijedi da je time definirana bijekcija $\varphi : A \to \mathbb{Q}$ koja je sličnost. Q.E.D.

Prije iskaza teorema o uređajnoj karakterizaciji skupa $\mathbb{R}$ uvodimo još jedan pojam.

Definicija 1.78. *Neka je $(B, \prec)$ linearno uređen skup. Za $A \subseteq B$ kažemo da je* **gust u** *B ako za sve $x, y \in B$, takve da je $x \prec y$, postoji $z \in A$ tako da vrijedi $x \prec z \prec y$.*

Skup $\mathbb{Q}$ je gust u $\mathbb{R}$. Zatim, skup $\{q + \sqrt{2} : q \in \mathbb{Q}\}$ je gust u $\mathbb{R}$.

Lema 1.79. *Neka je $(B, \prec)$ linearno uređen skup koji nema ni najveći ni najmanji element. Neka je $A \subseteq B$ podskup koji je gust u B. Tada A nema ni najmanji ni najveći element, te je A gust skup.*

Teorem 1.80. *(Uređajna karakterizacija skupa $\mathbb{R}$).*
Neka je $(B, \prec)$ linearno uređen skup koji ima sljedeća svojstva:

a) nema ni najveći ni najmanji element;

b) postoji prebrojiv $A \subseteq B$ koji je gust u B;

c) za svaki neprazan podskup od B koji je odozgo omeđen postoji supremum u B.

Tada je skup $(B, \prec)$ sličan sa $(\mathbb{R}, <)$.

Dokaz prethodnog teorema dan je kao rješenje zadatka 4.

Zadaci.

1. Dokažite da je skup svih realnih algebarskih brojeva sličan sa skupom $\mathbb{Q}$.

2. Dokažite da je skup $\langle 0, 1] \cup \langle 5, 8\rangle$ sličan sa skupom $\mathbb{R}$.

3. Dokažite lemu 1.79.
   Rješenje. Pretpostavimo da je $a \in A$ najveći. Po pretpostavci leme skup B nema ni najveći ni najmanji element pa postoji $x \in B$ takav da je $a \prec x$. Pošto je skup A gust u B tada postoji $b \in A$ tako da vrijedi $a \prec b \prec x$. No, to je nemoguće jer je po pretpostavci a najveći element u skupu A. Dokažimo još da je skup A gust. Neka su $x, y \in A$ takvi da $x \prec y$. Posebno su $x, y \in B$. Pošto je skup A gust u B tada postoji $z \in A$ takav da $x \prec z \prec y$.

4. Dokažite teorem o uređanoj karakterizaciji skupa $\mathbb{R}$.
   Rješenje. Iz leme 1.79. slijedi da skup A zadovoljava uvjete teorema o uređajnoj karakterizaciji skupa $\mathbb{Q}$, pa imamo $A \simeq \mathbb{Q}$. Neka je $f : A \to \mathbb{Q}$ neka sličnost. Sada ćemo sličnost f proširiti na skup B.

   Tvrdnja 1. Za svaki $x \in B$ skup $\{f(a) : a \in A,\ a \preceq x\}$ je neprazan i omeđen odozgo.
   Dokaz tvrdnje 1. Neka je $x \in B$ proizvoljan. Pošto po pretpostavci teorema skup B nema najmanji element tada postoji $x' \in B$ takav da je $x' \prec x$. Pošto je skup A gust u X tada postoji $a_0 \in A$ takav da je $x' \prec a_0 \prec x$. Iz toga slijedi $f(a_0) \in \{f(a) : a \in A,\ a \preceq x\}$, tj. promatrani skup je neprazan.

   Dokažimo sada da je skup $\{f(a) : a \in A,\ a \preceq x\}$ omeđen odozgo za svaki $x \in B$. Neka je $x \in B$ proizvoljan, ali fiksiran. Po pretpostavci teorema skup B nema najveći element pa postoji $x' \in B$ takav da je $x \prec x'$. Pošto je A gust skup u B tada postoji $a_0 \in A$ takav da je $x \prec a_0 \prec x'$. Tada za svaki $a \in A$, takav

da je $a \preceq x$, vrijedi $a \prec a_0$. Pošto je f sličnost tada je $f(a) < f(a_0)$ za svaki $a \preceq x$. To znači da je $f(a_0)$ jedna gornja međa skupa $\{f(a) : a \in A,\ a \preceq x\}$. Time je dokazana tvrdnja 1.

Iz dokazane tvrdnje 1 slijedi da je za svaki $x \in B$ dobro definiran realan broj:

$$\sup\{f(a)\ :\ a \in A,\ a \preceq x\}.$$

Pošto je supremum u linearno uređenom skupu jedinstven tada slijedi da je dobro definirana funkcija $F : B \to \mathbb{R},\ F(x) = \sup\{f(a)\ :\ a \in A,\ a \preceq x\}$.

Tvrdnja 2. Vrijedi: $F|_A = f$.
Dokaz tvrdnje 2. Neka je $a_0 \in A$ proizvoljan, ali fiksiran. Tada za svaki $a \in A$, takav da je $a \preceq a_0$, vrijedi $f(a) \leq f(a_0)$. To znači da je $f(a_0)$ jedna gornja međa skupa $\{f(a) : a \in A,\ a \preceq a_0\}$. Tvrdimo da je $f(a_0)$ supremum skupa $\{f(a) : a \in A,\ a \preceq a_0\}$, tj. najmanja gornja međa. Neka je $y \in \mathbb{R}$ neka gornja međa skupa $\{f(a) : a \preceq a_0, a \in A\}$. Tada za svaki $a \in A$, takav da je $a \preceq a_0$, vrijedi $f(a) \leq y$. Posebno je $f(a_0) \leq y$. Time je tvrdnja 2 dokazana.

Tvrdnja 3. Funkcija $F : B \to \mathbb{R}$ je rastuća i injekcija.
Dokaz tvrdnje 3. Neka su $x_1, x_2 \in B$ takvi da vrijedi $x_1 \prec x_2$. Po definiciji funkcije F imamo

$$F(x_1) = \sup\{f(a) : a \in A,\ a \preceq x_1\} \ \text{ i } \ F(x_2) = \sup\{f(a) : a \in A,\ a \preceq x_2\}.$$

Pošto je $x_1 \prec x_2$ tada je očito $\{f(a) : a \in A,\ a \preceq x_1\} \subseteq \{f(a) : a \in A,\ a \preceq x_2\}$. Iz toga odmah slijedi $\sup\{f(a) : a \in A,\ a \preceq x_1\} \preceq \sup\{f(a) : a \in A,\ a \preceq x_2\}$, tj. $F(x_1) \leq F(x_2)$. Lako je vidjeti da mora vrijediti $F(x_1) \prec F(x_2)$. Time je tvrdnja 3 dokazana.

Tvrdnja 4. Funkcija F je surjekcija.
Dokaz tvrdnje 4. Neka je $y \in \mathbb{R}$ proizvoljan. Očito je skup $\mathbb{Q}_y = \{q \in \mathbb{Q} : q \leq y\}$ neprazan i omeđen odozgo. Tada je i skup $f^{-1}[\mathbb{Q}_y]$ omeđen odozgo. Iz pretpostavke c) teorema slijedi da za skup $f^{-1}[\mathbb{Q}_y]$ postoji supremum. Neka je $x = \sup f^{-1}[\mathbb{Q}_y]$. Tvrdimo da je $F(x) = y$. Označimo $A_x := \{a \in A : a \preceq x\}$. Očito je $f^{-1}[\mathbb{Q}_y] \subseteq A_x$. Dokažimo obratnu inkluziju. Neka je $a \in A_x$ proizvoljan. Tada postoji $x' \in f^{-1}[\mathbb{Q}_y]$ takav da vrijedi $a \preceq x' \preceq x$. Iz toga slijedi $f(a) \leq f(x') \preceq y$, a onda $a \in f^{-1}[\mathbb{Q}_y]$. Dakle, vrijedi $f^{-1}[\mathbb{Q}_y] = A_x$, pošto je očito $y = \sup \mathbb{Q}_y$. Iz toga odmah slijedi $F(x) = y$.

1.8 Dobro uređeni skupovi

U ovoj točki razmatrat ćemo posebnu klasu linearno uređenih skupova: dobro uređene skupove. Oni su nam najvažniji za daljnja proučavanja jer su ordinalni bro-

jevi posebne vrste dobro uređenih skupova. Propozicije i teoremi, koje ćemo ovdje dokazati, omogućit će nam da dokazi svojstava ordinalnih brojeva budu jednostavniji.

Definicija 1.81. *Za parcijalno uređen skup $(A, <)$ kažemo da je* **dobro uređen** *ako svaki njegov neprazni podskup sadrži najmanji element.*

Uočite da je tu važno da smo prilikom definicije parcijalno uređenog skupa zahtijevali irefleksivnost relacije. Uočite da je svaki dobro uređen skup ujedno i linearno uređen.

Primjer 1.82. *Svaki konačan skup koji je linearno uređen je i dobro uređen skup. Skup $\mathbb{N}$ s prirodnim uređajem je dobro uređen skup. Skupovi $\mathbb{Q}$, $\mathbb{Z}$ i $\mathbb{R}$ s prirodnim uređajem nisu dobro uređeni skupovi.*

Sada nizom lema i korolara navodimo svojstva dobro uređenih skupova.

Lema 1.83. *Neka je $(A, <)$ dobro uređen skup, te $f : A \to A$ injekcija koja čuva uređaj. Tada za svaki $x \in A$ vrijedi $x \leq f(x)$.*

Dokaz. Pretpostavimo suprotno, tj. da postoji $a \in A$ takav da vrijedi $f(a) < a$. Tada je skup $C = \{x \in A : f(x) < x\}$ neprazan. Neka je $a_0 \in C$ najmanji element skupa C. Iz definicije skupa C slijedi $f(a_0) < a_0$. Pošto funkcija f čuva uređaj i injekcija je, tada vrijedi $f(f(a_0)) < f(a_0)$. Iz definicije skupa C slijedi $f(a_0) \in C$. Time dobivamo kontradikciju (a_0 je najmanji element skupa C, a po drugoj strani $f(a_0) < a_0$ i $f(a_0) \in C$). Q.E.D.

Važno je naglasiti da smo prethodni dokaz proveli promatrajući "prvu iznimku", odnosno primijenili smo indukciju na dobro uređenom skupu.

Korolar 1.84. *Dobro uređen skup ne može biti sličan svom početnom komadu.*

Dokaz. Neka je $(A, <)$ dobro uređen skup i $x_0 \in A$ proizvoljan. Ako je $p_A(x_0) = \emptyset$ tada je očito da skup A i taj početni komad nisu slični.

Neka je $p_A(x_0) \neq \emptyset$, te pretpostavimo da je $f : A \to p_A(x_0)$ sličnost. Iz prethodne leme 1.83. slijedi da je $x_0 \leq f(x_0)$. To je nemoguće jer je $f(x_0) \in p_A(x_0)$, pa vrijedi $f(x_0) < x_0$. Q.E.D.

Korolar 1.85. *Različiti početni komadi dobro uređenog skupa nisu slični.*

Dokaz. Neka je $(A, <)$ dobro uređen skup i $x_1, x_2 \in A$ različiti. Radi određenosti neka je $x_1 < x_2$. Tada je $p_A(x_1) \subseteq p_A(x_2)$. Pošto je $p_A(x_2)$ dobro uređen skup, te vrijedi $p_A(x_1) = p_{p_A(x_2)}(x_1)$, tražena tvrdnja slijedi iz prethodnog korolara 1.84. Q.E.D.

Napominjemo da tvrdnja prethodnog korolara općenito ne vrijedi za linearno uređene skupove. Primjerice za linearno uređen skup $\mathbb{R}$ imamo $p_{\mathbb{R}}(0) = \langle -\infty, 0\rangle \simeq \langle -\infty, 1\rangle = p_{\mathbb{R}}(1)$.

Korolar 1.86. *Dobro uređen skup ne može biti sličan podskupu nekog svog početnog komada.*

Dokaz. Neka je $(A, <)$ neprazan dobro uređen skup, $x_0 \in A$ i $B \subseteq p_A(x_0)$. Ako je $B = \emptyset$ tada tvrdnja korolara očito vrijedi. Promotrimo sada slučaj kada je $B \neq \emptyset$. Ako bi $f : A \to B$ bila sličnost tada iz leme 1.83. slijedi $x_0 \leq f(x_0)$. To je nemoguće jer za svaki $y \in B$ vrijedi $y < x_0$. Q.E.D.

Želimo napomenuti da dobro uređen skup može biti sličan nekom svom podskupu. Primjerice dobro uređen skup $\mathbb{N}$ je sličan sa svojim podskupom $2\mathbb{N}$.

Korolar 1.87. *Sličnost između dobro uređenih skupova je jedinstvena.*

Dokaz. Neka su $(A, <)$ i $(B, \prec)$ slični dobro uređeni skupovi. Neka su $f : A \to B$ i $g : A \to B$ dvije sličnosti. Neka je $a \in A$ proizvoljan. Očito vrijedi $p_A(a) \simeq p_B(f(a))$ i $p_A(a) \simeq p_B(g(a))$, a onda $p_B(f(a)) \simeq p_B(g(a))$. Iz korolara 1.85. slijedi $f(a) = g(a)$. Q.E.D.

Sada izričemo princip transfinitne indukcije koji je jedno od najmoćnijih sredstava za dokazivanje u teoriji skupova.

Princip transfinitne indukcije:
Neka je $(A, <)$ linearno uređen skup i $B \subseteq A$ koji ima sljedeće svojstvo:

$$(\forall x \in A)(p_A(x) \subseteq B \Rightarrow x \in B) \qquad (*)$$

Tada je $B = A$.

Primijetimo da za svaki neprazan dobro uređen skup A podskup B, koji ima svojstvo $(*)$, nužno sadrži najmanji element skupa A (ako je a_0 najmanji element skupa A tada je $p_B(a_0) = \emptyset \subseteq B$).

Zaključivanje po principu transfinitne indukcije općenito ne važi za linearno uređene skupove. Primjerice uzmemo li $A = \mathbb{Z}$, a $B = 2\mathbb{Z}$, tada je lako vidjeti da je ispunjen uvjet $(*)$. No, $\mathbb{Z} \neq 2\mathbb{Z}$.

Sljedeći teorem govori da princip transfinitne indukcije karakterizira dobro uređene skupove.

Teorem 1.88. *Neka je $(A, <)$ linearno uređen skup. Skup A ima najmanji element i za A vrijedi princip transfinitne indukcije ako i samo ako skup A je dobro uređen.*

Dokaz. Pretpostavimo prvo da je A dobro uređen skup. Neka je $B \subseteq A$ takav da za svaki $x \in A$ vrijedi da $p_A(x) \subseteq B$ povlači $x \in B$, ali $B \neq A$. Neka je a_0 najmanji element skupa $A \setminus B$. Ako je $y \in p_A(a_0)$ tada je očito $y \in B$, pa time imamo da vrijedi $p_A(a_0) \subseteq B$. Sada iz pretpostavljenog svojstva skupa B slijedi $a_0 \in B$, što je kontradikcija s činjenicom $a_0 \in A \setminus B$.

Pretpostavimo sada da je A linearno uređen skup koji ima najmanji element i za koji važi princip transfinitne indukcije. Pretpostavimo još da A nije dobro uređen skup. Neka je B neprazni podskup od A koji nema najmanji element. Definiramo skup C sa $C = \{x \in A \ : \ (\forall y \in B)x < y\}$. Primijetimo prvo da $C \neq \emptyset$ jer najmanji element skupa A pripada skupu C. Pretpostavimo da je $z \in A$ takav da je $p_A(z) \subseteq C$. Tada za svaki $x \in p_A(z)$ i svaki $y \in B$ vrijedi $x < y$. Budući da po pretpostavci skup B ne sadrži najmanji element, tada $z \notin B$. Tada za svaki $y \in B$ vrijedi $z < y$, pa $z \in C$. No, pretpostavili smo da za skup A vrijedi princip transfinitne indukcije, pa je $C = A$. Tako smo dobili $B \subseteq A = C$ i $(\forall x \in C)(\forall y \in B)x < y$, što je nemoguće. Q.E.D.

Teorem 1.89. *(Teorem o usporedivosti dobro uređenih skupova)*
Neka su $(A, <)$ i $(B, \prec)$ dobro uređeni skupovi. Tada vrijedi točno jedno od sljedećeg:

a) $A \simeq B$;

b) postoji jedinstveni $a \in A$ takav da vrijedi $p_A(a) \simeq B$;

c) postoji jedinstveni $b \in B$ takav da vrijedi $A \simeq p_B(b)$.

Dokaz. Ako je $A = \emptyset$ ili $B = \emptyset$ tada tvrdnja teorema očito vrijedi. Promatramo slučaj kada je $A \neq \emptyset$ i $B \neq \emptyset$. Neka je

$$A' = \{a \in A : \text{ postoji } b \in B \text{ takav da } \ p_A(a) \simeq p_B(b)\}$$

$$B' = \{b \in B : \text{ postoji } a \in A \text{ takav da } \ p_A(a) \simeq p_B(b)\}$$

Primijetimo prvo da su to neprazni skupovi, jer označimo li sa a_0 najmanji element skupa A, odnosno sa b_0 najmanji element od B, tada imamo $p_A(a_0) = \emptyset = p_B(b_0)$. Očito su A' i B' dobro uređeni skupovi, te vrijedi $A' \simeq B'$.

Neka je $a' \in A'$ proizvoljan. Tada iz definicije skupa A' slijedi da postoji $b \in B$ i $f : p_A(a') \to p_B(b)$ sličnost. Ako je $a \in A$ takav da je $a < a'$ tada je očito $p_A(a) \simeq p_B(f(a))$, pa je $a \in A'$. Iz toga slijedi da je $A' = A$ ili postoji $a \in A$ takav da je $A' = p_A(a)$ (ako je $A \neq A'$ tada uzemo a najmanji element skupa $A \setminus A'$). Analogno zaključujemo za skup B'. Iz toga slijedi da su moguća sljedeća četiri slučaja:

a) $A' = A$ i $B' = B$

b) $A' = A$ i postoji $b \in B$ takav da $B' = p_B(b)$

c) postoji $a \in A$ takav da $A' = p_A(a)$ i $B' = B$

d) postoji $a \in A$ takav da $A' = p_A(a)$ i postoji $b \in B$ takav da $B' = p_B(b)$

No, slučaj d) je nemoguć, jer iz $A' \simeq B'$, te $A' = p_A(a)$ i $B' = p_B(b)$ slijedi da je $a \in A'$ $(= p_A(a))$, što je nemoguće. Q.E.D.

Definicija 1.90. *Kažemo da je parcijalno uređen skup $(A, <)$ dobro utemeljen ako ne postoji niz (x_n) u skupu A tako da za svaki $n \in \mathbb{N}$ vrijedi $x_{n+1} < x_n$.*

Očito je svaki dobro uređen skup i dobro utemeljen. No, obrat ne vrijedi. Primjerice svaki dvočlani skup čiji elementi nisu usporedivi je dobro utemeljen, ali nije dobro uređen. Sada iskazujemo aksiom dobre utemeljenosti koji ćemo često koristiti u sljedećem poglavlju.

Aksiom dobre utemeljenosti

$$\forall x(x \neq \emptyset \rightarrow \exists y(y \in x \wedge y \cap x = \emptyset)).$$

Ovaj aksiom zapravo govori da je svaki skup dobro utemeljen u odnosu na relaciju $\in$. Iz aksioma dobre utemeljenosti slijedi da ne postoji skup x za koji bi postojao beskonačni niz skupova (x_n) tako da vrijedi: $\ldots \in x_2 \in x_1 \in x$. Odatle pak posebno slijedi da ne postoji skup x za kojeg bi vrijedilo $x \in x$.

Zadaci

1. Dokažite da za linearno uređene skupove ne vrijedi analogon Cantor, Schröder, Bernsteinovog teorema, tj. nađite primjere linearno uređenih skupova A i B, tako da je A sličan nekom podskupu skupa B i da je B sličan nekom podskupu skupa A, ali A nije sličan s B. Vrijedi li analogon Cantor-Bernsteinovog teorema za dobro uređene skupove?

2. Neka je $(A, <)$ linearno uređen skup. Dokažite da je skup A konačan ako i samo ako su skupovi $(A, <)$ i $(A, <^{-1})$ dobro uređeni. (Sa $<^{-1}$ je označena inverzna relacija relacije $<$).

3. Dokažite da ne postoji proširenje relacije $<$ sa skupa $\mathbb{R}$ na skup $\mathbb{C}$ koje bi imalo sljedeća svojstva:

   a) za sve $z \neq 0$ vrijedi $z < 0$ ili $0 < z$;

   b) ako je $0 < z_1$ i $0 < z_2$ tada je $0 < z_1 \cdot z_2$;

   c) ako je $z_1 < 0$ i $z_2 < 0$ tada je $z_1 + z_2 < 0$.

   Rješenje. Pretpostavimo da takvo proširenje postoji, i označimo ga isto s $<$. Promotrimo slučajeve obzirom na 0 i i, te 0 i $-i$. Ako je $0 < i$ tada zbog uvjeta b) imamo $0 < i \cdot i$, tj. $0 < -1$. Dakle, mora biti $i < 0$. Ako je $0 < -i$ tada zbog uvjeta b) imamo $0 < (-i) \cdot (-i)$, tj. $0 < -1$. To znači da je $-i < 0$. Time imamo da je $i < 0$ i $-i < 0$. Primjenom uvjeta c) dobivamo $0 < 0$, tj. kontradikciju.

4. Za podskup A parcijalno uređenog skupa $(S, <)$ kažemo da je kofinalan u S ako vrijedi $(\forall x \in S)(\exists a \in A)(x \leq a)$. Dokažite da svaki linearno uređen skup sadrži kofinalan dobro uređen skup.

Poglavlje 2

Aksiomatska teorija skupova

U prethodnom poglavlju naučili smo osnovne pojmove kao što su: konačan i beskonačan skup, (ne)prebrojiv skup, kardinalnost i dobro uređeni skupovi. Tu smo već uočili probleme prilikom definicije kardinalnog broja. Zapravo govorili smo o kardinalnosti, a ne o kardinalnim brojevima. Naučili smo da svi beskonačni skupovi nemaju istu kardinalnost, te smo proučavali operacije kako bi dobili nove kardinalnosti. No, ne znamo što je kardinalni broj. To ćemo znati kada definiramo ordinalne brojeve. Imamo barem tri razloga za definiciju ordinalnog broja:

a) Moramo odgovoriti što je "nivo" u kumulativnoj hijerarhiji.

b) Prije smo već bili postavili problem kako definirati beskonačne ordinalne brojeve.

c) Pomoću ordinalnih brojeva definirat ćemo kardinalne brojeve.

Ordinalni brojevi su neki dobro uređeni skupovi, pri čemu je relacija uređaja zapravo relacija "biti element", tj. relacija $\in$. Kardinalni brojevi su neki posebni ordinalni brojevi. (Svaki konačni ordinalni broj je kardinalni broj.)

Želimo naglasiti da bez obzira na naslov ovog poglavlja *Aksiomatska teorija skupova* sada se nećemo baviti aksiomima i formalnim dokazima. Naslov poglavlja je takav jer egzistencija objekata koje promatramo može biti dokazana pomoću aksioma teorije `ZF`.

Naveli smo većinu aksioma teorije `ZF` koji su nam bili potrebni kako bi definirali neke pojmove, odnosno dokazali neke tvrdnje. Preostalo je još iskazati aksiom beskonačnosti i shemu aksioma zamjene. Nakon definicije ordinalnog broja, navest ćemo teoreme enumeracije i rekurzije. Usput ćemo navesti kako uvesti, odnosno strogo definirati, skupove brojeva $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ i $\mathbb{R}$.

Definirat ćemo aritmetiku ordinalnih brojeva, tj. zbrajanje, množenje i potenciranje. Posebnu pažnju posvetit ćemo kardinalnim brojevima. Na samom kraju razmatrat ćemo aksiom izbora.

2.1 Prirodni brojevi

Često se može čuti da je teorija skupova osnova matematike. Razlog tome je činjenica da se mnogi matematički objekti mogu definirati u teoriji ZF, te se tu mogu dokazati njihova osnovna svojstva. Mi ćemo sada definirati skupove brojeva. Na taj način želimo ilustrirati tvrdnju da je teorija skupova osnova matematike. Prvo ćemo definirati prirodne brojeve. Kasnije ćemo vidjeti da su prirodni brojevi zapravo konačni ordinalni brojevi. Dakle, prirodni brojevi su nam i dobra motivacija prije razmatranja ordinalnih brojeva.

Definicija 2.1. *Za skup x kažemo da je* **induktivan** *ako vrijedi $\emptyset \in x$ i za svaki $y \in x$ vrijedi $(y \cup \{y\}) \in x$. Sa $Ind(x)$ označavamo sljedeću formulu:*

$$\emptyset \in x \ \wedge \ \forall y(y \in x \to y \cup \{y\} \in x).$$

Kažemo da je skup x **prirodan broj** *ako za svaki induktivan skup y vrijedi $x \in y$. Sa $Pri(x)$ označavamo formulu $\forall y(Ind(y) \to x \in y)$.*

Navedimo nekoliko primjera prirodnih brojeva: $\emptyset$, $\{\emptyset\}$, $\{\emptyset, \{\emptyset\}\}$.

Može se pokazati da iz do sada navednih aksioma teorije ZF ne možemo dokazati egzistenciju skupa svih prirodnih brojeva. To nam omogućava sljedeći aksiom.

Aksiom beskonačnosti: Postoji induktivan skup, tj. formalno

$$\exists x\Big(\emptyset \in x \wedge \forall y\Big(y \in x \to (y \cup \{y\}) \in x\Big)\Big).$$

Ako je F neka tvrdnja[1] u daljnjem tekstu ćemo sa $\mathtt{ZF} \vdash F$ označavati činjenicu da je tvrdnja F dokaziva u teoriji ZF.

Kako bi barem malo ilustrirali netrivijalnost navedene definicije prirodnih brojeva u teoriji ZF, dokazat ćemo da je aksiom matematičke indukcije dokaziv u teoriji ZF. Prvi korak prema tome je sljedeća lema.

Lema 2.2. *Klasa $\omega = \{x : Pri(x)\}$ je skup, tj. vrijedi*

$$\mathtt{ZF} \vdash \exists! x \forall y(y \in x \leftrightarrow Pri(y)).$$

Skup ω je najmanji induktivan skup.

Dokaz leme je dan kao rješenje zadatka 1 na strani 61. Ako je x prirodan broj tada sa $x + 1$ označavamo skup $x \cup \{x\}$. Ako je $x \in \omega$ tada je očito i $x + 1 \in \omega$, tj. $x + 1$ je također prirodan broj.

[1] Točnije, F je proizvoljna formula teorije ZF. Ovdje nećemo strogo definirati pojam formule. Grubo govoreći F može biti sastavljena od varijabli, simbola $=$ i $\in$, bulovskih veznika i kvantifikatora. Za strogu definiciju pojma formule vidite primjerice [38].

Teorem 2.3. *U teoriji ZF je dokaziva shema aksioma matematičke indukcije. Odnosno, ako je $F(x)$ proizvoljna formula tada vrijedi:*

$$\mathtt{ZF} \vdash \Big(F(\emptyset) \wedge \forall x(Pri(x) \wedge F(x) \to F(x+1)) \Big) \to \forall x(Pri(x) \to F(x)).$$

Dokaz prethodnog teorema dan je kao rješenje zadatka 2 na strani 62. Uočite da nismo naveli da je aksiom matematičke indukcije dokaziv u teoriji ZF, jer je aksiom matematičke indukcije jedna formula logike drugog reda (detalje o tome možete pogledati primjerice u [38]).

Za nekoliko prvih prirodnih brojeva uvodimo oznake: $0 := \emptyset$, $1 := \{\emptyset\}$, $2 := \{0, 1\}$ i $3 := \{0, 1, 2\}$. Na taj način možemo definirati i 17, ali malo teže broj 3 234. No, uočite da to ne može biti definicija prirodnih brojeva, odnosno skupa prirodnih brojeva (dobra rasprava o tome je dana u knjizi [16].)

Sada definiramo pojam tranzitivnog skupa koji će nam trebati prilikom definicije ordinalnih brojeva.

Definicija 2.4. *Kažemo da je skup x tranzitivan ako vrijedi $\forall y \forall z(y \in z \in x \ \to y \in x)$. Sa $Trans(x)$ označavamo formulu $\forall y \forall z(y \in z \ \wedge \ z \in x \ \to y \in x)$.*

Osnovne primjere tranzitivnih skupova navodimo u sljedećoj propoziciji. Dokaz propozicije je dan kao rješenje zadatka 5 na strani 62.

Propozicija 2.5. *Svaki prirodan broj je tranzitivan skup. Skup ω je tranzitivan.*

Korolar 2.6. *Ako je x prirodan broj i $y \in x$ tada je i y prirodan broj.*

Neka je $x = \{\{\emptyset\}\}$. Taj skup nije tranzitivan jer vrijedi $\emptyset \in \{\emptyset\} \in x$, ali ne i $\emptyset \in x$. Skupovi $\{\emptyset, \{\{\emptyset\}\}\}$ i $\{\emptyset, \{\{\{\emptyset\}\}\}\}$ također nisu tranzitivni.

Definicija 2.7. *Neka su m i n prirodni brojevi. Kažemo da je m* **manji** *od n, i pišemo $m < n$, ako vrijedi $m \in n$.*

Lako je dokazati da je upravo definirani uređaj na skupu ω linearan.

Kako bismo na skupu ω mogli definirati zbrajanje i množenje, a i druge funkcije, moramo prvo dokazati Dedekindov teorem rekurzije. Taj teorem, a i njegov dokaz, dobra je motivacija za teorem rekurzije koji ćemo izreći kasnije. Prisjetimo se nekih primjera rekurzivnih definicija funkcija. Faktorijeli se rekurzivno definiraju ovako:

$$\begin{aligned} 0! &= 1 \\ (n+1)! &= n! \cdot (n+1) \end{aligned}$$

Zatim, Fibonaccijev niz se rekurzivno definira ovako:

$$\begin{aligned} F_0 &= 1 \\ F_1 &= 1 \\ F_{n+2} &= F_n + F_{n+1} \end{aligned}$$

Sigurno ste na takve definicije već toliko navikli da se i pomalo čudnim čini pitanje jesu li te definicije dobre, odnosno postoje li jedinstvene funkcije koje to zadovoljavaju. Dedekindov teorem rekurzije upravo govori da rekurzivnim definicijama zadajemo jedinstvene funkcije na skupu ω.

U iskazu i dokazu Dedekindovog teorema koristimo da za svaki prirodan broj n vrijedi $n = \{m : m \in \omega \text{ i } m < n\}$ (za dokaz te činjenice vidi zadatak 4 na strani 62). Ako je $f : \omega \to S$ neka funkcija i $n \in \omega$ tada nam $f|n$ označava restrikciju funkcije f na skup n.

Teorem 2.8. *(Dedekindov teorem rekurzije)*
Neka je S proizvoljan skup, te neka je $\Phi = \{f|$ postoji $n \in \omega$ tako da $f : n \to S\}$. Neka je $F : \Phi \to S$ proizvoljna funkcija. Tada postoji jedinstvena funkcija $\varphi : \omega \to S$ takva da za svaki $n \in \omega$ vrijedi $\varphi(n) = F(\varphi|n)$.

Ideja dokaza je vrlo jednostavna. Očito mora vrijediti $\varphi(0) = F(\emptyset)$ (uočite da je $\emptyset \in \Phi$, jer funkciju $f : 0 \to \omega$ možemo poistovjetiti sa $\emptyset$). Zatim, ako s f_1 označimo funkciju koja nuli pridružuje $F(\emptyset)$ tada mora vrijediti $\varphi(1) = F(f_1)$. Ako s f_2 označimo funkciju definiranu na $\{0, 1\}$ s $f_2(0) = F(\emptyset)$ i $f_2(1) = F(f_1)$ tada mora vrijediti $\varphi(2) = F(f_2)$. Analogno dalje.

Upravo ta jednostavnost je razlog zašto se teorem prihvaća u svakodnevnoj praksi bez da se postavlja pitanje njegovog dokaza. No, važno je uočiti da zapravo nije glavno pitanje je li tvrdnja teorema istinita, već može li se dokaz provesti u teoriji ZF.

Detaljan dokaz Dedekindovog teorema rekurzije dan je kao rješenje zadatka 14. U sljedećem korolaru izričemo verziju Dedekindovog teorema koja je sličnija rekurzivnim definicijama na koje smo navikli. Ponekad se u literaturi upravo ta verzija naziva Dedekindov teorem rekurzije.

Korolar 2.9. *Neka je S proizvoljan skup i $s_0 \in S$, te $h : S \to S$ proizvoljna funkcija. Tada postoji jedinstvena funkcija $\varphi : \omega \to S$ za koju vrijedi:*

$$\begin{aligned} &\varphi(0) = s_0 \\ &\varphi(m+1) = h(\varphi(m)), \quad \textit{za svaki } m \in \omega. \end{aligned}$$

Primjer 2.10. *Pokažimo sada kako možemo definirati zbrajanje prirodnih brojeva u teoriji ZF. Tvrdimo da je pomoću jednakosti: $x + 0 = x$ i $x + (y + 1) = (x + y) + 1$, definirana jedinstvena funkcija. Neka je Φ skup svih funkcija čije su domene prirodni brojevi, a kodomena je ω. Za svaki $m \in \omega$ promatramo funkciju $F_m : \Phi \to \omega$ tako da je $F_m(\emptyset) = m$, a za $f \in \Phi$, čija je domena $n + 1$, definiramo $F_m(f) = f(n) + 1$. Tada iz Dedekindovog teorema slijedi da postoji jedinstvena funkcija $\varphi_m : \omega \to \omega$, tako da za*

svaki $n \in \omega$ vrijedi $\varphi_m(n) = F_m(\varphi_m|n)$. Tada imamo $\varphi_m(0) = F_m(\varphi_m|0) = F_m(\emptyset) = m$, te $\varphi_m(n+1) = F_m(\varphi_m|n+1) = \varphi_m(n) + 1$. Neka je funkcija $+ : \omega \times \omega \to \omega$ definirana sa $m + n = \varphi_m(n)$. Lako je vidjeti da vrijedi: $m + 0 = m$ i $m + (n+1) = (m+n) + 1$.

Primjer 2.11. *Koristeći se Dedekindovom teorem rekurzije možemo dokazati egzistenciju Fibonaccijevog niza u teoriji ZF. U tu svrhu prvo definiramo funkciju $F : \Phi \to \omega$. Za $f \in \Phi$, čija je domena neki $n \in \omega$, definiramo:*

$$F(f) = \begin{cases} 0, & \text{ako je } n = 0, \\ 1, & \text{ako je } n = 1, \\ f(m) + f(m+1), & \text{pri čemu je } n = m + 2 \end{cases}$$

Iz Dedekindovog teorema rekurzije slijedi da postoji jedinstvena funkcija φ tako da za svaki $n \in \omega$ vrijedi $\varphi(n) = F(\varphi|n)$. Tada imamo:

$$\begin{aligned} \varphi(0) &= F(\emptyset) = 0 \\ \varphi(1) &= F(\varphi|_1) = 1 \\ \varphi(n) + \varphi(n+1) &= F(\varphi|_{n+2}) = \varphi(n+2) \end{aligned}$$

Očito je $(\varphi(n))_{n\in\omega}$ Fibonaccijev niz.

Kao što smo bili dokazali da u teoriji ZF za skup ω vrijedi shema aksioma matematičke indukcije (vidi teorem 2.3.), tako bi na analogan način mogli dokazati da skup ω zadovoljava i sve ostale **Peanove aksiome** koje sada navodimo:

1) $n + 1 \neq 0$

2) $n + 1 = m + 1 \Rightarrow n = m$

3) $n + 0 = n$

4) $m + (n+1) = (m+n) + 1$

5) $n \cdot 0 = 0$

6) $m \cdot (n+1) = m \cdot n + m$

Primijetite da smo dokazali da u ZF vrijede svojstva 1) i 2). Aksiomi 3)–6) su rekurzivne definicije zbrajanja i množenja. Iz Dedekindovog teorema rekurzije slijedi da su time stvarno definirane jedinstvene funkcije.

Zadaci

1. Dokažite lemu 2.2.
   Dokaz. Aksiom beskonačnosti jednostavno tvrdi da postoji barem jedan induktivan skup. Označimo sa I jedan induktivan skup. Očito vrijedi $\{x : Pri(x)\} = \{x : x \in I \ \wedge \ Pri(x)\}$, jer po definiciji prirodnih brojeva imamo da je svaki prirodan broj element proizvoljnog induktivnog skupa. Sada iz sheme aksioma separacije slijedi da je ω skup. Jedinstvenost skupa ω slijedi iz aksioma ekstenzionalnosti. Očito je $\omega \subseteq I$, tj. ω je najmanji induktivan skup.

2. Dokažite teorem 2.3.
   Dokaz. Neka je $F(x)$ proizvoljna formula tako da vrijedi

   $$\texttt{ZF} \vdash F(\emptyset) \wedge \forall x(Pri(x) \wedge F(x) \rightarrow F(x+1)) \qquad (*)$$

   Označimo $X = \{x : Pri(x) \text{ i } \texttt{ZF} \vdash F(x)\}$. Iz leme 2.2. slijedi da je tada $X = \{x : x \in \omega \text{ i } \texttt{ZF} \vdash F(x)\}$. Iz sheme aksioma separacije slijedi da je X skup.

   Pošto po pretpostavci $(*)$ posebno vrijedi $\texttt{ZF} \vdash F(\emptyset)$ tada imamo $\emptyset \in X$. Zatim, ako je $x \in X$ tada je $x \in \omega$ i vrijedi $\texttt{ZF} \vdash F(x)$. Iz pretpostavke $(*)$ tada slijedi $\texttt{ZF} \vdash F(x+1)$, tj. imamo da je $x+1 \in X$. To znači da je X induktivan skup.

   Po definiciji svaki induktivan skup sadrži svaki prirodan broj. Posebno imamo da za svaki prirodan broj x vrijedi $x \in X$, a onda iz definicije skupa X slijedi da vrijedi $\texttt{ZF} \vdash F(x)$.

3. Ako je $m \in \omega$ dokažite da je tada $m \subseteq \omega$.

4. Primjenom sheme aksioma matematičke indukcije dokažite da za svaki $n \in \omega$ vrijedi $n = \{m \ : \ m \in \omega \ \text{ i } \ m < n\}$.

5. Dokažite propoziciju 2.5.
   Dokaz. Želimo dokazati da vrijedi $\texttt{ZF} \vdash \forall x(Pri(x) \rightarrow Trans(x))$. Tu tvrdnju dokazujemo indukcijom, tj. primjenom dokazanog teorema 2.3. Iz aksioma praznog skupa slijedi da vrijedi $\texttt{ZF} \vdash y \in z \in \emptyset \rightarrow y \in \emptyset$, tj. $\texttt{ZF} \vdash Trans(\emptyset)$.

   Pretpostavimo da je neki prirodan broj x tranzitivan, te neka imamo $y \in z \in x+1$. Tada je $z \in x \cup \{x\}$, tj. $z \in x$ ili $z = x$. Lako je vidjeti da u oba slučaja vrijedi $y \in x$. Pošto je $x \subseteq x+1$ tada imamo i traženu tvrdnju, tj. $y \in x+1$.

   Dokažimo sada da je ω tranzitivan skup. Moramo dokazati da $y \in z \in \omega$ povlači $y \in \omega$. Iz leme 2.2. slijedi da je ta tvrdnja ekvivalentna sa: $Pri(z) \wedge y \in z \in \omega$ povlači $y \in \omega$. Posljednja tvrdnja se lako dokaže indukcijom po z.

6. Ako je x prirodan broj i $y \in x$ dokažite da je tada i y prirodan broj.
   Dokaz. Pošto je x prirodan broj tada $x \in \omega$. Pošto je ω tranzitivan skup tada iz $y \in x \in \omega$ slijedi $y \in \omega$. Sada iz $\omega = \{z : Pri(z)\}$ slijedi da je y prirodan broj.

7. Ako je $m \in \omega$ i $m \neq 0$ dokažite da tada postoji $n \in \omega$ tako da vrijedi $m = n+1$.

8. Dokažite da vrijede osnovna svojstva (komutativnost, asocijativnost, distributivnost, ...) operacija zbrajanja i množenja na skupu ω.

9. Dokažite da je relacija $\in$ na skupu ω linearni uređaj.

10. Ako je $m \in \omega \ \text{ i } \ m \neq 0$ dokažite da tada vrijedi $0 < m$.

11. Ako su $m, n \in \omega$ i $m < n$ dokažite da je tada $m+1 < n$ ili $m+1 = n$.

12. Dokažite da svaki neprazan podskup od ω ima najmanji element.

13. Neka su $m, n \in \omega$ i $m < n$. Dokažite da skupovi m i n nisu ekvipotentni.

14. Dokažite Dedekindov teorem rekurzije.
Rješenje. Označimo s $\mathcal{G}$ skup svih funkcija g čija je domena neki $n \in \omega$ a kodomena skup S, te za svaki $m < n$ vrijedi $g(m) = F(g|m)$. (Funkcije koje pripadaju skupu $\mathcal{G}$ možemo zamišljati kao konačne aproksimacije tražene funkcije φ.) Dokaz provodimo po koracima, dokazujući redom tvrdnje.

Tvrdnja 1. Ako su $g, h \in \mathcal{G}$ takve da je $g : m \to S$ i $h : n \to S$, te je $m < n$, tada vrijedi $g = h|m$.
Tvrdnju je lako dokazati indukcijom po $i < m$. (Dokaz koraka indukcije: $g(i) = F(g|i) = F(h|i) = h(i) = (h|m)(i)$.)

Tvrdnja 2. Za svaki $m \in \omega$ postoji funkcija $g \in \mathcal{G}$ takva da je $m \in Dom(g)$.
Dokaz se provodi indukcijom po m. Za $m = 0$ možemo uzeti funkciju $g : 1 \to S$ definiranu s $g(0) = F(\emptyset)$. Pretpostavimo da za neki $m \in \omega$ postoji funkcija $g \in \mathcal{G}$ takva da je $m \in Dom(g)$. Ako je $m + 1 \in Dom(g)$ tada je dokaz gotov. Pretpostavimo zato da $m + 1 \notin Dom(g)$. Definiramo funkciju $h : (m + 2) \to S$ sa:

$$h(i) = \begin{cases} g(i), & \text{ako je } i \in m + 1, \\ F(g), & \text{ako je } i = m + 1. \end{cases}$$

Lako je provjeriti da je $h \in \mathcal{G}$. Time je tvrdnja 2. dokazana.

Sada definiramo $\varphi = \bigcup_{g \in \mathcal{G}} g$. Dokažimo prvo da je φ funkcija.
Neka $(a, b),\ (a, c) \in \varphi$. Iz definicije φ slijedi da postoje funkcije $g, h \in \mathcal{G}$ tako da vrijedi $g(a) = b$ i $h(a) = c$. Radi određenosti možemo pretpostaviti da je $Dom(g) = m$ i $Dom(h) = n$, te je $m < n$. Iz dokazane tvrdnje 1. slijedi $g \subseteq h$. Zato je $b = c$.

Očito je $Dom(\varphi) \subseteq \omega$. Pokažimo i obratnu inkluziju. Neka je $m \in \omega$ proizvoljan. Tada iz dokazane tvrdnje 2. slijedi da postoji funkcija $g \in \mathcal{G}$ takva da je $m \in Dom(g)$. Tada je očito $m \in Dom(\varphi)$. Time smo dokazali $\omega = Dom(\varphi)$.

Primijetimo da je slika funkcije φ sadržana u skupu S. (Ako je $m \in \omega$ tada prema dokazanoj tvrdnji 2. slijedi da možemo izabrati funkciju $g \in \mathcal{G}$ tako da vrijedi $m \in Dom(g)$. Pošto je kodomena funkcije g upravo skup S, te je $\varphi(m) = g(m)$, tada je $\varphi(m) \in S$).

Dokažimo sada da za svaki $m \in \omega$ vrijedi $\varphi(m) = F(\varphi|m)$. Neka je $m \in \omega$ proizvoljan. Tada iz dokazane tvrdnje 2. slijedi da postoji $g \in \mathcal{G}$ tako da je $m \in Dom(g)$. Iz dokazane tvrdnje 1. slijedi da za svaki $i < m$ vrijedi $i \in Dom(g)$, te je $\varphi(i) = g(i)$. Tada imamo: $\varphi(m) = g(m) = F(g|m) = F(\varphi|m)$.

Preostalo je još dokazati jedinstvenost funkcije φ. Pretpostavimo da je $\theta : \omega \to S$ funkcija takva da za svaki $m \in \omega$ vrijedi $\theta(m) = F(\theta|m)$. Indukcijom po m dokazujemo da vrijedi $\varphi(m) = \theta(m)$. Redom imamo: $\varphi(0) = F(\varphi|0) = F(\emptyset) = F(\theta|0) = \theta(0)$. Neka je $m \in \omega$ koji ima svojstvo da za svaki $i < m$ vrijedi $\varphi(i) = \theta(i)$. Tada imamo: $\varphi(m) = F(\varphi|m) = F(\theta|m) = \theta(m)$.

15. Dokažite korolar 2.9.
Rješenje. Neka je Φ skup svih funkcija čija je domena neki prirodan broj, a kodomena je skup S. Definiramo funkciju $F : \Phi \to S$ tako da je $F(\emptyset) = s_0$, a za $f \in \Phi$ takvu da je $Dom(f) = n + 1$ definiramo $F(f) = h(f(n))$. Iz Dedekindovog teorema rekurzije slijedi da postoji funkcija $\varphi : \omega \to S$ takva da za svaki $m \in \omega$ vrijedi $\varphi(m) = F(\varphi|_m)$. Tada imamo $\varphi(0) = F(\varphi|0) = F(\emptyset) = s_0$, te $\varphi(m + 1) = F(\varphi|m + 1) = h(\varphi(m))$.

16. Primjenom Dedekindovog teorema rekurzije dokažite da postoji jedinstvena funkcija f na $\omega \times \omega$ koja zadovoljava:

$$\begin{aligned} f(x, 0) &= 0 \\ f(x, y + 1) &= f(x, y) \ + \ x \end{aligned}$$

17. Dokažite da su svi Peanovi aksiomi istiniti na ω.

18. Ackermannova funkcija je definirana sljedećim uvjetima:

$$f(0, n) = n + 1$$

$$f(n + 1, 0) = f(m, 1)$$

$$f(m + 1, n + 1) = f(m, f(m + 1, n))$$

Dokažite da za sve $m, n \in \omega$ vrijedi:

$$n < f(m, n)$$

$$f(m, n) < f(m, n + 1)$$

$$f(m, n + 1) \leq f(m + 1, n)$$

$$f(m, n) < f(m + 1, n)$$

Nije nimalo jednostavno dokazati egzistenciju Ackermannove funkcije koristeći Dedekindov teorem rekurzije. No, to je jednostavno napraviti primjenom teorema rekurzije koji ćemo kasnije navesti.

2.2 Skupovi brojeva $\mathbb{Z}$, $\mathbb{Q}$ i $\mathbb{R}$

U ovoj točki prvo ćemo pokazati kako pomoću skupa ω možemo definirati skup cijelih brojeva i operacije na njemu. Zatim ćemo pomoću skupa $\mathbb{Z}$ definirati skup racionalnih brojeva $\mathbb{Q}$. Nizom zadataka definirat ćemo skup $\mathbb{R}$ na kraju ove točke.

Cijeli brojevi

U daljnjim razmatranjima pretpostavljamo da su dokazana sva svojstva operacija na skupu ω koja ćemo upotrebljavati. Prije nego što napišemo formalne definicije pokušat ćemo objasniti glavne ideje prilikom uvođenja skupa cijelih brojeva. Cijeli broj x poistovjetit ćemo sa skupom svih uređenih parova (m, n) prirodnih brojeva za koje vrijedi $x = m - n$. Primjerice broj -1 je jednak skupu $\{(n, n+1) : n \in \omega\}$, a broj nula je jednak skupu $\{(n, n) : n \in \omega\}$. Općenito, cijeli broj definirat ćemo kao svaki skup uređenih parova prirodnih brojeva čija je razlika konstantna. U tu svrhu nam treba relacija ekvivalencije. Imamo mali problem. Na skupu ω nije definirana razlika svaka dva elementa, pa ne možemo definirati relaciju $\sim$ na skupu $\omega \times \omega$ sa: $(m_1, n_1) \sim (m_2, n_2)$ ako i samo ako $m_1 - n_1 = m_2 - n_2$. No, uvjet $m_1 - n_1 = m_2 - n_2$ je ekvivalentan sa $m_1 + n_2 = n_1 + m_2$, pa smo izbjegli oduzimanje. Zapišimo sada to sve formalno.

Definicija 2.12. *Na skupu $\omega \times \omega$ definiramo binarnu relaciju $\sim$ sa:*

$$(m_1, n_1) \sim (m_2, n_2) \quad \textit{ako i samo ako} \quad m_1 + n_2 = n_1 + m_2$$

Lako je provjeriti da je to relacija ekvivalencije. Za uređeni par (m, n) sa $[(m, n)]$ označavamo pripadnu klasu ekvivalencije. Skup cijelih brojeva $\mathbb{Z}$ definiramo kao skup svih klasa ekvivalencije relacije $\sim$, tj. $\mathbb{Z} = \omega \times \omega / \sim$.

Primijetimo da s ovakvom definicijom skupa $\mathbb{Z}$ ne vrijedi $\omega \subseteq \mathbb{Z}$. Iz tog razloga svaki prirodan broj n poistovjećujemo sa cijelim brojem $[(n, 0)]$, pa je onda svaki prirodan broj ujedno i cijeli broj.

Na skupu $\mathbb{Z}$ sada želimo definirati osnovne operacije. Prije formalne definicije pokušat ćemo objasniti glavne ideje. Ako su $[(m_1, n_1)]$ i $[(m_2, n_2)]$ cijeli brojevi tada te klase zapravo predstavljaju $m_1 - n_1$ i $m_2 - n_2$. To znači da bi suma cijelih brojeva $[(m_1, n_1)]$ i $[(m_2, n_2)]$ trebala predstavljati $(m_1 - n_1) + (m_2 - n_2)$, što je jednako $(m_1 + m_2) - (n_1 + n_2)$. No, ovaj zadnji izraz je predstavljen s klasom ekvivalencije $[(m_1 + m_2,\ n_1 + n_2)]$. Na sličan način produkt cijelih brojeva $[(m_1, n_1)]$ i $[(m_2, n_2)]$ trebao bi predstavljati $(m_1 - n_1) \cdot (m_2 - n_2)$, što je jednako $(m_1 \cdot m_2 + n_1 \cdot n_2) - (m_1 \cdot n_2 + n_1 \cdot m_2)$. Zadnji izraz je predstavljen s klasom ekvivalencije $[(m_1 \cdot m_2 + n_1 \cdot n_2,\ m_1 \cdot n_2 + n_1 \cdot m_2)]$. Na sasvim analogni način se može opravdati definicija relacije uređaja na skupu $\mathbb{Z}$.

Definicija 2.13. *Na skupu $\mathbb{Z}$ definiramo zbrajanje, množenje, suprotni element i relaciju uređaja na sljedeći način:*

$$\begin{aligned}
[(m_1,n_1)] \;+\; [(m_2,n_2)] &= [(m_1+m_2,\; n_1+n_2)] \\
[(m_1,n_1)]\cdot[(m_2,n_2)] &= [(m_1\cdot m_2+n_1\cdot n_2,\; m_1\cdot n_2+n_1\cdot m_2)] \\
-[(m,n)] &= [(n,m)] \\
[(m_1,n_1)] \;<\; [(m_2,n_2)] &\quad \textit{ako i samo ako}\quad m_1+n_2<n_1+m_2
\end{aligned}$$

Naravno, sada bi prvo trebalo provjeriti da upravo definirane operacije i relacija uređaja ne ovise o izboru reprezentanata, što je rutinski posao. Nije teško dokazati razna svojstva upravo definiranih operacija na skupu $\mathbb{Z}$ koristeći svojstva operacija na skupu ω. Primjerice komutativnost zbrajanja cijelih brojeva dokazujemo ovako:

$$\begin{aligned}
[(m_1,n_1)] \;+\; [(m_2,n_2)] &= [(m_1+m_2,n_1+n_2)] \;=\; [(m_2+m_1,n_2+n_1)] \\
&= [(m_2,n_2)] \;+\; [(m_1,n_1)]
\end{aligned}$$

Racionalni brojevi.

Sada pretpostavljamo da su dokazana sva svojstva operacija na skupu $\mathbb{Z}$ koja ćemo upotrebljavati. Kao i u prethodnoj situaciji, prije nego što napišemo formalne definicije pokušat ćemo objasniti glavne ideje prilikom uvođenja skupa racionalnih brojeva. Racionalni broj x ćemo poistovjetiti sa skupom svih uređenih parova (p,q) cijelih brojeva za koje vrijedi $x=p/q$. Primjerice broj $1/2$ je jednak skupu $\{(n,2n) : n\in\omega\setminus\{0\}\}$, a broj nula je jednak skupu $\{(0,n) : n\in\omega\setminus\{0\}\}$. Općenito, racionalni broj definirat ćemo kao svaki skup uređenih parova cijelih brojeva čiji je kvocijent konstantan. U tu svrhu nam treba relacija ekvivalencije. Pošto na skupu $\mathbb{Z}$ nije definiran kvocijent svaka dva elementa tada ne možemo definirati relaciju $\sim$ na skupu $\mathbb{Z}\times(\omega\setminus\{0\})$ sa: $(p_1,q_1)\sim(p_2,q_2)$ ako i samo ako $p_1/q_1=p_2/q_2$. No, uvjet $p_1/q_1=p_2/q_2$ je ekvivalentan sa $p_1\cdot q_2=q_1\cdot p_2$, pa smo izbjegli dijeljenje.

Definicija 2.14. *Na skupu $\mathbb{Z}\times(\omega\setminus\{0\})$ definiramo binarnu relaciju $\sim$ sa:*

$$(p_1,q_1)\sim(p_2,q_2)\quad \textit{ako i samo ako}\quad p_1\cdot q_2=q_1\cdot p_2$$

Lako je provjeriti da je to relacija ekvivalencije. Za uređeni par (p,q) sa $[(p,q)]$ označavamo pripadnu klasu ekvivalencije. Skup racionalnih brojeva $\mathbb{Q}$ definiramo kao skup svih klasa ekvivalencije relacije $\sim$, tj. $\mathbb{Q}=\mathbb{Z}\times(\omega\setminus\{0\})/\sim$.

Uz ovakve definicije očito ne vrijedi $\mathbb{Z}\subseteq\mathbb{Q}$. Iz tog razloga cijeli broj m možemo poistovjetiti s racionalnim brojem $[(m,1)]$, pa tada vrijedi $\mathbb{Z}\subseteq\mathbb{Q}$. Operacije na skupu $\mathbb{Q}$ definiramo tako da "simuliramo" zbrajanje, odnosno množenje razlomaka.

Definicija 2.15. *Na skupu $\mathbb{Q}$ definiramo zbrajanje, množenje, suprotni element i relaciju uređaja na sljedeći način:*

$$\begin{aligned}
[(p_1,q_1)] \ + \ [(p_2,q_2)] &= [(p_1\cdot q_2 \ + \ p_2\cdot q_1,\ q_1\cdot q_2)] \\
[(p_1,q_1)]\cdot[(p_2,q_2)] &= [(p_1\cdot p_2,\ q_1\cdot q_2)] \\
-[(p,q)] &= [(-p,q)] \\
[(p_1,q_1)] < [(p_2,q_2)] &\qquad \textit{ako i samo ako} \qquad p_1\cdot q_2 \ < p_2\cdot q_1
\end{aligned}$$

Lako je dokazati da prethodne definicije ne ovise o izboru reprezentanata, te da definirane operacije i relacije imaju "očekivana" svojstva (komutativnost, asocijativnost, distributivnost, ...)

Neke napomene o definiciji skupa realnih brojeva su dane u zadacima koji slijede. Više detalja o uvođenju skupova brojeva možete naći u [11], [23] i [28].

Zadaci

1. Na skupu $\omega\times\omega$ definiramo binarnu relaciju $\sim$ sa:

   $$(m_1,n_1)\sim(m_2,n_2) \ \text{ ako i samo ako } \ m_1+n_2=n_1+m_2$$

   Dokažite da je $\sim$ relacija ekvivalencije.

2. Dokažite da definicije zbrajanja, množenja, suprotnog elementa i relacije uređaja na skupu $\mathbb{Z}$ ne ovise o izboru reprezentanta klase ekvivalencije.

3. Dokažite osnovna svojstva operacija zbrajanja i množenja na skupu $\mathbb{Z}$ (komutativnost, asocijativnost, ...)
   Uputa. Vidi [23].

4. Dokažite da je relacija uređaja na skupu $\mathbb{Z}$ irefleksivna, tranzitivna i linearni uređaj, te je kompatibilna sa zbrajanjem i množenjem.

5. Na skupu $\mathbb{Z}\times(\omega\setminus\{0\})$ definiramo binarnu relaciju $\sim$ sa:

   $$(p_1,q_1)\sim(p_2,q_2) \ \text{ ako i samo ako } \ p_1\cdot q_2=q_1\cdot p_2$$

   Dokažite da je to relacija ekvivalencije.

6. Dokažite da definicije zbrajanja, množenja, suprotnog elementa i relacije uređaja na skupu $\mathbb{Q}$ ne ovise o izboru reprezentanta klase ekvivalencije.

7. Dokažite osnovna svojstva operacija zbrajanja i množenja na skupu $\mathbb{Q}$ (komutativnost, asocijativnost, ...)
Uputa. Vidi [23].

8. Primjenom skupa racionalnih brojeva možemo definirati skup realnih brojeva. Ovdje opisujemo Dedekindovu konstrukciju koja se bazira na rezovima (vidi [11] i [28]). Neka su $\emptyset \neq A, B \subseteq \mathbb{Q}$ takvi da je $A \cup B = \mathbb{Q}$, $A \cap B = \emptyset$, te za svaki $a \in A$ i svaki $b \in B$ vrijedi $a < b$. Tada uređeni par (A, B) nazivamo **rez** skupa $\mathbb{Q}$. Ako je (A, B) rez skupa $\mathbb{Q}$ takav da skup A nema najveći element, tada skup A nazivamo realni broj. Skup svih realnih brojeva označavamo sa $\mathbb{R}$. Na skupu $\mathbb{R}$ definiramo operacije i relacije:

   zbrajanje: $A + C = \{r + q : r \in A,\ q \in C\}$

   uređaj: $A < C$ ako i samo ako $A \subset C$

   suprotni element: $-A = \{s \in \mathbb{Q} : (\exists r \in \mathbb{Q} \setminus A)(s < -r)\}$

   Primjerice ako je $A = \langle -\infty, 3\rangle \cap \mathbb{Q}$ tada je $3 = \sup A$, pa je $-3 = \inf\{-x : x \in A\}$. Iz toga slijedi da je po definiciji $-A = \langle -\infty, -3\rangle \cap \mathbb{Q}$.

   Dokažite da je zbrajanje realnih brojeva komutativno i asocijativno. Zatim, dokažite da je upravo definirana relacija uređaja irefleksivna i tranzitivna, te da su svaka dva realna broja usporediva.

9. Na skupu $\mathbb{R}$ definiramo redom:

   skup pozitivnih realnih brojeva: $\mathbb{R}^+ = \{A \in \mathbb{R} : 0 \in A\}$

   "realna" nula: $0_{\mathbb{R}} = \langle -\infty, 0\rangle \cap \mathbb{Q}$

   množenje na $\mathbb{R}^+$
   ako $X, Y \in \mathbb{R}^+$ tada definiramo $X \cdot Y = \{r \cdot s : 0 \leq r \in X \text{ i } 0 \leq s \in Y\} \cup 0_{\mathbb{R}}$

   $0_{\mathbb{R}} \cdot X = X \cdot 0_{\mathbb{R}} = 0_{\mathbb{R}}$, za svaki $X \in \mathbb{R}$

   Na skupu $\mathbb{R}$ definirajte množenje za slučajeve kada $X \in \mathbb{R}^+$ i $Y \notin \mathbb{R}^+$, te kada $X, Y \notin \mathbb{R}^+$. Dokažite da je množenje na skupu $\mathbb{R}$ komutativna i asocijativna operacija. Dokažite da je realan broj $0_{\mathbb{R}}$ neutralan element za zbrajanje. Zatim, dokažite da za svaki realan broj A vrijedi $A + (-A) = 0_{\mathbb{R}}$.

10. Označimo skup $\langle -\infty, 1\rangle \cap \mathbb{Q}$ sa $1_{\mathbb{R}}$. Za svaki $A \in \mathbb{R} \setminus \{0_{\mathbb{R}}\}$ definiramo recipročan broj A^{-1} ovako:

    a) ako $A \in \mathbb{R}^+$ tada definiramo $A^{-1} = \{s \in Q : \exists r \notin A(s < r^{-1})\}$;

    b) ako $-A \in \mathbb{R}^+$ tada definiramo $A^{-1} = -(-A)^{-1}$

Dokažite da za svaki $A \in \mathbb{R} \setminus \{0_{\mathbb{R}}\}$ vrijedi $A \cdot A^{-1} = 1_{\mathbb{R}}$.

11. Dokažite da je $\mathbb{R}$ uređeno Arhimedovo polje, te da je realno zatvoreno polje (tj. svaki polinom neparnog stupnja s koeficijentima iz $\mathbb{R}$ ima nultočku u $\mathbb{R}$).

12. Dokažite da za svaki $\emptyset \neq S \subseteq \mathbb{R}$, koji je odozgo ograničen, postoji supremum. (Uputa: $\sup S = \cup S$.)

13. Cantorova konstrukcija skupa realnih brojeva koristi Cauchyjeve nizove. Za niz (a_n) racionalnih brojeva kažemo da je Cauchyjev, ili kratko C–niz, ako vrijedi:

$$(\forall \epsilon > 0)(\exists n_0 \in \mathbb{N})(\forall m, n \geq n_0)(|a_n - a_m| < \epsilon)$$

Na skupu svih racionalnih C–nizova definiramo relaciju $\sim$ ovako:

$$(a_n) \sim (b_n) \text{ ako i samo ako } \lim_{n\to\infty}(a_n - b_n) = 0.$$

Lako je provjeriti da je $\sim$ relacija ekvivalencije. Svaku klasu ekvivalencije nazivamo realni broj. Definirajte operacije zbrajanja i množenja za tako definirane realne brojeve, te dokažite osnovna svojstva tih operacija.

2.3 Ordinalni brojevi

Već u osnovnoj školi uči se da svaki prirodan broj može biti promatran s dva aspekta. Prirodan broj određuje koliko čega ima ili određuje redno mjesto. Nas ovdje upravo zanimaju redni brojevi: prvi, drugi, treći, ... No, ne zanimaju nas samo konačni redni brojevi već bismo željeli govoriti i o beskonačnim rednim brojevima.

Što znače redni brojevi? Prvi po redu znači da ispred njega nema nitko. Drugi znači da je ispred njega samo jedan, itd. Iz tog razloga se redni brojevi u teoriji skupova definiraju na sljedeći način:

$$\begin{aligned} 0. &= \emptyset \\ 1. &= \{\emptyset\} \\ 2. &= \{0.,\ 1.\} = \{\emptyset,\ \{\emptyset\}\} \\ 3. &= \{0.,\ 1.,\ 2.\} \\ &\vdots \end{aligned}$$

Kasnije ćemo vidjeti da je svaki ordinalni broj zapravo dobro uređeni skup x koji ima svojstvo da za svaki $a \in x$ vrijedi $a = p_x(a)$ (vidi lemu 2.18.).

Neka vas ne zbunjuje početak definicije $0. = \emptyset$ (prazan skup!). Kao što se primjerice definira $0! = 1$ tako se i ovdje mora imati početak definicije. Napominjemo da u literaturi nije uobičajno koristiti oznake 0., 1., 2., 3., ..., već se jednostavno piše 0, 1, 2, 3, ... U daljnjem tekstu mi ćemo također konačne redne brojeve označavati s 0, 1, 2, 3, ...

Definicija 2.16. *Za skup x kažemo da je* **ordinalni broj** *ako je x tranzitivan skup i $(x, \in)$ je dobro uređen skup.*

Uočite da je u definiciji ordinalnog broja x dovoljno zahtijevati da je x tranzitivan skup, te je relacija $\in$ linearni uređaj na skupu x. Irefleksivnost relacije $\in$, te svojstvo da svaki neprazni podskup od x ima najmanji element, slijedi iz aksioma dobre utemeljenosti.

Primijetite da zahtjev da je x tranzitivan skup ne povlači da je relacija $\in$ na skupu x tranzitivna. Obrat također nije općenito istinit.

Primjer 2.17. *a) Prazan skup $\emptyset$, te $\{\emptyset\}$ i $\{\emptyset, \{\emptyset\}\}$ su ordinalni brojevi. Svaki prirodan broj je ordinalni broj. Skup ω je ordinalni broj.*

b) Skupovi $\{\{\emptyset\}\}$ i $\{\{\{\emptyset\}\}, \emptyset\}$ nisu ordinalni brojevi, jer nisu tranzitivni skupovi.

c) Svaki tranzitivan skup nije ordinalni broj. Skup $\{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}\}$ je tranzitivan, jer je očito svaki njegov element ujedno i njegov podskup. No, relacija $\in$ nije linearni uređaj, jer imamo $\emptyset \notin \{\{\emptyset\}\}$ i $\{\{\emptyset\}\} \notin \emptyset$.

Obično ćemo ordinalne brojeve označavati malim grčkim slovima: α, β, γ, δ, ...
Ako su α i β ordinalni brojevi tada definiramo:

$$\alpha < \beta \text{ ako i samo ako } \alpha \in \beta$$

Ako je α ordinalni broj i $x \in \alpha$ tada sa $p_\alpha(x)$ označavamo skup $\{y : y \in \alpha \text{ i } y \in x\}$.

Lema 2.18. *Ako je α ordinalni broj i $\beta \in \alpha$ tada je i β ordinalni broj, te vrijedi $\beta = p_\alpha(\beta)$.*

Dokaz. Pošto je α tranzitivan skup tada je $\beta \subseteq \alpha$, pa je $(\beta, \in)$ dobro uređen skup, jer je restrikcija relacije dobrog uređaja ponovo dobar uređaj. Dokažimo da je β tranzitivan skup. Neka $x \in y \in \beta$. Pošto tada $x \in y \in \beta \in \alpha$, te je α tranzitivan skup, tada imamo $x, y, \beta \in \alpha$. No, relacija $\in$ je tranzitivna na skupu α pošto je $(\alpha, \in)$ dobro uređen skup. Tada iz $x \in y \in \beta$ slijedi $x \in \beta$.
Dokažimo sada da vrijedi $\beta = p_\alpha(\beta)$. Očito vrijedi: $x \in \beta$ ako i samo ako $x \in \alpha$ i $x \in \beta$ (pošto je α tranzitivan skup). Ovo posljednje je ekvivalentno sa $x \in p_\alpha(\beta)$. Q.E.D.

Lema 2.19. *Ako su α i β ordinalni brojevi takvi da je $\alpha \simeq \beta$ tada vrijedi $\alpha = \beta$.*

Dokaz. Neka je $f : \alpha \to \beta$ sličnost. (Bili smo dokazali da je sličnost između dobro uređenih skupova jedinstvena; vidi korolar 1.87.) Želimo dokazati da je f identiteta. Pretpostavimo suprotno, tj. da postoji $z \in \alpha$ takav da je $f(z) \neq z$. Tada je skup $A = \{z \in \alpha : f(z) \neq z\}$ neprazan. Pošto je A neprazan podskup dobro uređenog skupa α tada skup A sadrži najmanji element. Označimo najmanji element skupa A sa a.

Tvrdimo da vrijedi $a = f(a)$. (Time će biti dobivena kontradikcija, jer je $a \in A$.) U tu svrhu dokazujemo obje inkluzije. Dokažimo prvo da vrijedi $a \subseteq f(a)$. Neka je $x \in a$ proizvoljan. Tada imamo $x \in a \in \alpha$, pa zbog tranzitivnosti skupa α slijedi $x \in \alpha$. Pošto je domena funkcije f skup α, tada je definirano $f(x)$. Sada iz $x \in a$, te pošto je f sličnost, imamo $f(x) \in f(a)$. No, a je najmanji element skupa α koji ima svojstvo $f(a) \neq a$, a pošto $x \in a$, tada $f(x) = x$. Time smo dokazali da vrijedi $x \in f(a)$.
Dokažimo obratnu inkluziju. Neka je $y \in f(a)$ proizvoljan. Posebno je $y \in \beta$, a pošto je funkcija f surjekcija, tada postoji $x \in \alpha$ takav da je $y = f(x)$. Time imamo $f(x) \in f(a)$. Pošto je funkcija f sličnost, tj. f^{-1} čuva uređaj, tada imamo $x \in a$. Pošto je a najmanji element skupa α za koji vrijedi $a \neq f(a)$, te imamo $x \in a$, tada vrijedi $x = f(x)$. Konačno, iz $y = f(x),\ x = f(x)$ i $x \in a$, slijedi $y \in a$. Q.E.D.

Propozicija 2.20. *(Linearnost uređaja na ordinalnim brojevima)*
Ako su α i β ordinalni brojevi tada vrijedi: $\alpha < \beta$ ili $\alpha = \beta$ ili $\beta < \alpha$.

Dokaz. Iz definicije ordinalnog broja znamo da su skupovi $(\alpha, \in)$ i $(\beta, \in)$ dobro uređeni. Iz teorema o usporedivosti dobro uređenih skupova, tj. teorema 1.89., slijedi da vrijedi jedno od:

a) $\alpha \simeq \beta$

b) postoji $x \in \alpha$ takav da je $p_\alpha(x) \simeq \beta$

c) postoji $y \in \beta$ takav da je $p_\beta(y) \simeq \alpha$.

Ako je $\alpha \simeq \beta$ tada iz prethodne leme 2.19. slijedi $\alpha = \beta$. Promotrimo sada slučaj b). Iz leme 2.18. znamo $x = p_\alpha(x)$, te x je ordinalni broj. Sada iz $x \simeq \beta$, te leme 2.19., slijedi $x = \beta$. Time imamo $\beta \in \alpha$, tj. $\beta < \alpha$. Analogno bi razmatrali slučaj c). Q.E.D.

Korolar 2.21. *Svaki skup ordinalnih brojeva je dobro uređen s relacijom $\in$.*
Svaki tranzitivan skup ordinalnih brojeva je ordinalan broj.

Sljedeći teorem je iznimno važan. On jednostavno govori da je svaki dobro uređen skup sličan jedinstvenom ordinalnom broju. To nam omogućava da definiramo pojam ordinalnog broja proizvoljnog dobro uređenog skupa. Zatim, taj teorem na neki način opravdava definiciju ordinalnog broja, tj. da je ordinalni broj stvarno pravi reprezentant klase svih međusobno sličnih dobro uređenih skupova.

Prije iskaza i dokaza teorema enumeracije navodimo posljednji aksiom (odnosno shemu aksioma!) Zermelo–Fraenkelove teorije skupova. To je shema aksioma zamjene. Prvo istaknimo jednu motivaciju za uvođenje sheme zamjene. Iz aksioma partitivnog skupa slijedi da možemo izgraditi sljedeći niz skupova:

$$A_1 = \mathcal{P}(\mathbb{N}), \quad A_2 = \mathcal{P}(A_1), \quad A_3 = \mathcal{P}(A_2), \ldots$$

No, može se pokazati da iz do sada navedenih aksioma ne možemo dokazati da je klasa $S = \{A_n : n \in \mathbb{N}\}$ skup. Iz tog se razloga dodaje još jedan aksiom, koji se intuitivno može izreći ovako:

ako je F skupovna operacija (preslikavanje F svakom skupu pridružuje jedinstveni skup), tada je za svaki skup u klasa $F[u]$ također skup.

Formalni zapis **sheme aksioma zamjene** je sljedeći:

$$\forall t_1 \ldots \forall t_k \Big(\quad \forall x \exists! y F(x, y, t_1, \ldots t_k) \rightarrow$$

$$\forall u \exists v \forall z \big(z \in v \leftrightarrow \exists w (w \in u \wedge F(w, z, t_1, \ldots, t_k)) \big) \Big),$$

gdje je F proizvoljna formula teorije ZF, te u i v su različite varijable koje su različite od x, y, z, $t_1, \ldots, t_k$ i w. U prvom dijelu aksioma je zapisana "funkcionalnost" formule F, tj. ističe se da nas zanimaju formule koje opisuju neku funkciju. Zatim se u drugom dijelu aksioma tvrdi da je slika skupa također skup (tj. ako je u skup tada je i slika skupa u, obzirom na funkciju koju definira formula F, također skup). Shemu aksioma zamjene koristit ćemo u dokazu sljedećeg teorema.

Teorem 2.22. *(Teorem enumeracije)*
Za svaki dobro uređeni skup $(A, <)$ postoji jedinstveni ordinalni broj α koji je sličan sa A.

Dokaz. Jedinstvenost slijedi direktno iz leme 2.19. Dokažimo sada da postoji traženi ordinalni broj. U tu svrhu prvo dokazujemo da ako za svaki početni komad dobro uređenog skupa A postoji ordinalni broj tada postoji ordinalni broj i za A, tj.:

$$(\forall a \in A)(\exists \alpha)(p_A(a) \simeq \alpha) \qquad \Rightarrow \qquad (\exists \beta)(A \simeq \beta) \tag{1}$$

Pretpostavimo da za svaki $a \in A$ postoji ordinalni broj $O(a)$ tako da vrijedi $p_A(a) \simeq O(a)$. Iz leme 2.19. slijedi da je za svaki $a \in A$ ordinalni broj $O(a)$ jedinstven. Označimo $O(A) = \{O(a) : a \in A\}$. Iz sheme aksioma zamjene slijedi da je $O(A)$ skup. Zatim, označimo s $O : A \rightarrow O(A)$ funkciju definiranu sa: $A \ni a \qquad \mapsto \qquad O(a)$. Dokazat ćemo da je $O(A)$ ordinalni broj koji je sličan skupu A, te da je funkcija O sličnost. Za svaki $a \in A$ sa $f_a : p_A(a) \rightarrow O(a)$ označimo sličnost između dobro uređenih skupova $p_A(a)$ i $O(a)$. (Prilikom razmatranja dobro uređenih skupova bili smo dokazali da je sličnost između sličnih dobro uređenih skupova jedinstvena; vidi korolar 1.87.).

Prvo dokažimo da je skup ordinalnih brojeva $O(A)$ ordinalni broj. Iz korolara 2.21. slijedi da je dovoljno dokazati da je skup $O(A)$ tranzitivan. Neka $y \in O(a) \in O(A)$. Pošto je $O(a)$ ordinalni broj tada iz leme 2.18. slijedi da je y ordinalni broj. Pošto je f_a surjekcija i $y \in O(a)$ tada postoji $x \in p_A(a)$ takav da je $y = f_a(x)$. Tada je očito restrikcija $f_a|_{p_A(x)} : p_A(x) \rightarrow y$ sličnost. Dakle, y je ordinalni broj koji je sličan nekom početnom komadu skupa A. Tada iz leme 2.19. slijedi da je $y \in O(A)$.

Dokažimo sada da je funkcija $O : A \rightarrow O(A)$ sličnost. Za to je dovoljno dokazati da za sve $x, y \in A$ vrijedi: $x < y$ ako i samo ako $O(x) \in O(y)$. Pretpostavimo prvo da

vrijedi $x < y$. Tada je $p_A(x) \subset p_A(y)$. Zatim, znamo $O(x) \simeq p_A(x)$ i $O(y) \simeq p_A(y)$. Pošto su $O(x)$ i $O(y)$ ordinalni brojevi tada iz propozicije 2.20. slijedi da vrijedi: $O(x) \in O(y)$ ili $O(x) = O(y)$ ili $O(y) \in O(x)$.

Ako $O(x) = O(y)$ tada imamo $p_A(x) \simeq p_A(y)$, što je nemoguće jer su to različiti početni komadi istog dobro uređenog skupa (to smo dokazali prilikom razmatranja dobro uređenih skupova; vidi korolar 1.85.).

Ako $O(y) \in O(x)$ tada iz leme 2.18. slijedi $p_{O(x)}(O(y)) = O(y)$. No, onda je $p_A(y)$ sličan nekom početnom komadu od $p_A(x)$. Pošto je $p_A(x) \subset p_A(y)$ tada bi imali da je dobro uređen skup $p_A(y)$ sličan podskupu nekog svog početnog komada, što je nemoguće zbog korolara 1.86.

Pretpostavimo sada da vrijedi $O(x) \in O(y)$. Po pretpostavci teorema je A dobro uređen skup pa vrijedi: $x < y$ ili $x = y$ ili $y < x$. Ako vrijedi $x = y$ tada imamo $O(x) = O(y)$ što je suprotno pretpostavci. Pretpostavimo sada da vrijedi $y < x$. Iz prethodno dokazane tvrdnje tada imamo $O(y) < O(x)$. Iz ovog posljednjeg i pretpostavke $O(x) < O(y)$ slijedi $O(x) < O(x)$, što je nemoguće. Time smo dokazali tvrdnju (1). Rezimirajmo: dokazali smo da ako je svaki početni komad dobro uređenog skupa sličan nekom ordinalnom broju tada je skup A sličan ordinalnom broju $O(A)$. Promotrimo li tvrdnju (1) vidimo da za dokaz teorema dovoljno dokazati još sljedeće: $(\forall a \in A)(\exists \alpha)(p_A(a) \simeq \alpha)$. Pretpostavimo suprotno, tj. da je skup

$$B = \{a \in A : \text{ ne postoji ordinalni broj } \alpha \text{ tako da } p_A(a) \simeq \alpha\}$$

neprazan. Time imamo da je B neprazan podskup dobro uređenog skupa A, pa sadrži najmanji element b. Označimo $C = p_A(b)$. Pošto je b najmanji element skupa B tada je za svaki $x \in C$ skup $p_C(x)$ sličan nekom ordinalnom broju, a skup C nije sličan niti jednom ordinalnom broju. No, to je nemoguće zbog upravo dokazane tvrdnje (1). Q.E.D.

Definicija 2.23. *Neka je A dobro uređeni skup. Jedinstveni ordinalni broj α za koji vrijedi $A \simeq \alpha$ nazivamo* **ordinalni broj skupa** *A, te ga označavamo s $o(A)$.*

Burali–Forti je dokazao da klasa svih ordinalnih brojeva prava klasa. To ističemo u sljedećoj propoziciji.

Propozicija 2.24. *(Burali–Fortijev paradoks)*
Klasa $On = \{\alpha : \alpha$ je ordinalni broj$\}$ je prava klasa.

Dokaz. Pretpostavimo da je On skup. Ako $\alpha \in \beta \in On$ tada iz leme 2.18. slijedi da je α ordinalni broj, tj. $\alpha \in On$. To znači da je On tranzitivan skup. Iz korolara 2.21. slijedi da je skup On ordinalni broj. No, tada vrijedi da je $On \in On$, što je nemoguće zbog aksioma dobre utemeljenosti. Q.E.D.

Cesare Burali–Forti, 1861.–1931.

Propozicija 2.25. *Neka je A neki skup ordinalnih brojeva. Tada vrijedi:*

a) $\bigcup_{\alpha\in A}\alpha$ *je ordinalni broj i najmanji je od svih ordinalnih brojeva koji su veći ili jednaki od svih elemenata iz A, tj.* $\bigcup_{\alpha\in A}\alpha = \sup A$*;*

b) $\bigcap_{\alpha\in A}\alpha$ *je ordinalni broj i najveći je od svih ordinalnih brojeva koji su manji ili jednaki od svih elemenata iz A, tj.* $\bigcap_{\alpha\in A}\alpha = \inf A$.

Kako bi mogli definirati ordinalne brojeve prve i druge vrste prvo ističemo sljedeću propoziciju.

Propozicija 2.26. *Za svaki ordinalni broj α skup $\alpha\cup\{\alpha\}$ je ordinalni broj, te je to neposredni sljedbenik od α. Ordinalni broj $\alpha\cup\{\alpha\}$ označavamo sa $\alpha+1$. Ako su α i β ordinalni brojevi za koje vrijedi $\alpha<\beta$ tada je $\alpha+1\leq\beta$.*

Definicija 2.27. *Za ordinalni broj α kažemo da je* **prve vrste** *ako postoji ordinalni broj β tako da vrijedi $\alpha=\beta+1$. Ako je ordinalni broj različit od nule, te nije prve vrste, tada kažemo da je* **druge vrste** *ili da je* **granični ordinalni broj**.

Svaki prirodni broj različit od nule je ordinalni broj prve vrste. Zatim, $\omega+1$ je ordinalni broj prve vrste. Ordinalni broj ω je najmanji granični ordinalni broj. (Za sada ne znamo niti jedan drugi granični ordinalni broj.)

Bili smo dokazali da za svaki dobro uređeni skup važi zaključivanje po principu transfinitne indukcije. Svaki ordinalni broj je dobro uređeni skup (u odnosu na relaciju $\in$), pa na ordinalne brojeve također možemo primijeniti princip transfinitne indukcije. Znamo da je svaki skup ordinalnih brojeva također dobro uređeni skup. No, iz Burali–Fortijevog paradoksa znamo da klasa On svih ordinalnih brojeva nije skup, pa spomenuti teorem o principu transfinitne indukcije ne možemo primijeniti na klasu svih ordinalnih brojeva. Sada ističemo da princip transfinitne indukcije vrijedi za klasu On, te da se taj dokaz može provesti u teoriji ZF. Dokaz je u biti sasvim analogan spomenutom teoremu o principu transfinitne indukcije za dobro uređene skupove.

Teorem 2.28. *(Transfinitna indukcija)*
Neka je $F(x)$ neka formula teorije ZF. Pretpostavimo da formula $F(x)$ ima sljedeće svojstvo:

$$\mathtt{ZF} \vdash \forall\alpha\Big(\big((\forall\beta < \alpha)F(\beta)\big) \Rightarrow F(\alpha) \Big).$$

(Sa α i β su označeni ordinalni brojevi).
Tada za svaki ordinalni broj α vrijedi $\mathtt{ZF} \vdash F(\alpha)$.

Sada navodimo teorem rekurzije koji će nam omogućiti da zbrajanje, množenje i potenciranje možemo definirati za sve ordinalne brojeve. Teorem rekurzije nije samo važan za definicije operacija na ordinalnim brojevima, već i za definiciju kumulativne hijerarhije, tj. za definiciju sljedeće skupovne operacije:

$$\alpha \mapsto V_\alpha = \{\mathcal{P}(V_\beta) : \beta < \alpha\}$$

Teorem rekurzije je generalizacija Dedekindovog teorema rekurzije za prirodne brojeve koji smo bili prije naveli. U teoremu govorimo o preslikavanjima koja su definirana za svaki ordinalni broj, tj. za svaki $\alpha \in On$. To znači da, strogo govoreći, ne promatramo funkcije, već skupovne operacije.

Želimo naglasiti da ovo nije teorem teorije ZF, već teorem koji govori o ZF. Dokaz teorema rekurzije je sasvim analogan dokazu Dedekindovog teorema rekurzije. Detalje dokaza možete primjerice vidjeti u [16].

Teorem 2.29. *(Teorem rekurzije)*
Neka je A granični ordinalni broj ili klasa On svih ordinalnih brojeva. Neka je S neka proizvoljna klasa. Neka je, zatim, $s_0 \in S$ i $G : S \to S$ proizvoljna skupovna operacija. Neka je

$$\Phi = \{f \mid \text{ postoji granični ordinalni broj } \beta \in A \text{ takav da je } f : \beta \to S\}.$$

Neka je $F : \Phi \to S$ proizvoljna skupovna operacija. Tada postoji jedinstvena skupovna operacija $\varphi : A \to S$ tako da za svaki $\beta \in A$ vrijedi

$$\varphi(\beta) = \begin{cases} s_0, & \text{ako je } \beta = 0, \\ G(\varphi(\gamma)), & \text{ako je } \beta = \gamma + 1, \\ F(\varphi|\beta), & \text{ako je } \beta \text{ granični ordinal} \end{cases}$$

Kao prvu primjenu teorema rekurzije dajemo definiciju kumulativne hijerarhije. Sa V označimo klasu svih skupova. Neka je $s_0 = \emptyset$, te skupovna operacija $G : V \to V$ neka je definirana sa $G(x) = \mathcal{P}(x)$. Zatim, neka je skupovna operacija $F : \Phi \to V$

definirana ovako: ako je $f \in \Phi$, čija je domena granični ordinalni broj β, tada je $F(f) = \bigcup_{\gamma<\beta} f(\gamma)$.

Iz teorema rekurzije slijedi da postoji jedinstvena skupovna operacija $\varphi : On \to V$ koja ima tražena svojstva. Za $\alpha \in On$ označimo $V_\alpha = \varphi(\alpha)$. Tada imamo:

$$V_0 = \varphi(0) = \emptyset,$$

$$V_{\alpha+1} = \varphi(\alpha+1) = G(\varphi(\alpha)) = \mathcal{P}(V_\alpha)$$

$$V_\alpha = \varphi(\alpha) = F(\varphi|\alpha) = \bigcup_{\beta<\alpha} \varphi(\beta) = \bigcup_{\beta<\alpha} V_\beta$$

što je upravo tražena definicija kumulativne hijerarhije.
Sada ćemo definirati zbrajanje, množenje i potenciranje ordinalnih brojeva.

Definicija 2.30. *Neka je α proizvoljan ordinalni broj. Iz teorema rekurzije slijedi da postoji jedinstvena skupovna operacija $\varphi_\alpha : On \to On$ tako da vrijedi:*

$$\varphi_\alpha(0) = \alpha$$
$$\varphi_\alpha(\beta+1) = \varphi_\alpha(\beta) + 1$$
$$\varphi_\alpha(\beta) = \sup\{\varphi_\alpha(\gamma) : \gamma < \beta\}, \quad \textit{ako je } \beta \textit{ granični ordinalni broj.}$$

Sada možemo definirati skupovnu operaciju $+ : On \times On \to On$ sa $\alpha + \beta = \varphi_\alpha(\beta)$. Odnosno, kratko možemo reći da primjenom teorema rekurzije slijedi da postoji jedinstvena skupovna operacija $+ : On \times On \to On$ koja ima sljedeća svojstva:

$$\alpha + 0 = \alpha$$
$$\alpha + (\beta+1) = (\alpha+\beta) + 1$$
$$\alpha + \beta = \sup\{\alpha + \gamma : \gamma < \beta\}, \quad \textit{ako je } \beta \textit{ granični ordinalni broj.}$$

Upravo definiranu skupovnu operaciju nazivamo **zbrajanje ordinalnih brojeva**.

Alternativna definicija zbrajanja ordinalnih brojeva dana je u zadataku 5 na strani 80. U sljedećoj propoziciji ističemo osnovna svojstva zbrajanja ordinalnih brojeva. Sva svojstva se dokazuju primjenom principa transfinitne indukcije i zadatka 5.

Propozicija 2.31. *(Svojstva zbrajanja ordinalnih brojeva)*
Neka su α, β i γ proizvoljni ordinalni brojevi. Tada vrijedi:

a) $0 + \alpha = \alpha$

b) $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$

c) Ako je $\alpha + \beta = \alpha + \gamma$ *tada je* $\beta = \gamma$

Napomena 2.32. *Posebno želimo istaknuti da zbrajanje ordinalnih brojeva općenito nije komutativno. Primjerice* $1+\omega = \sup\{1+n : n \in \omega\} = \omega$, *ali* $\omega + 1 \neq \omega$, *jer znamo da vrijedi* $\omega < \omega + 1$.

Općenito iz $\beta + \alpha = \gamma + \alpha$ *ne mora slijediti* $\beta = \gamma$ *(primjerice vrijedi* $1 + \omega = 2 + \omega$*).*

Definicija 2.33. *Primjenom teorema rekurzije slijedi da je s jednakostima koje slijede definirana jedinstvena skupovna operacija* $\cdot : On \times On \to On$*:*

$$\alpha \cdot 0 = 0$$

$$\alpha \cdot (\beta + 1) = \alpha \cdot \beta + \alpha$$

$$\alpha \cdot \beta = \sup\{\alpha \cdot \gamma : \gamma < \beta\}, \quad \textit{ako je } \beta \textit{ granični ordinalni broj.}$$

Skupovnu operaciju $\cdot$ *nazivamo* **množenje ordinalnih brojeva**.

Ekvivalentna definicija množenja ordinalnih brojeva dana je u zadataku 8 na strani 83. U sljedećoj propoziciji ističemo osnovna svojstva množenja ordinalnih brojeva. Sva svojstva se dokazuju primjenom principa transfinitne indukcije i zadatka 8.

Propozicija 2.34. *(Svojstva množenja ordinalnih brojeva)*
Neka su α, β *i* γ *proizvoljni ordinalni brojevi. Tada vrijedi:*

a) $\alpha \cdot 1 = 1 \cdot \alpha = \alpha$

b) $\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$

c) $\alpha \cdot (\beta \cdot \gamma) = (\alpha \cdot \beta) \cdot \gamma$

d) Ako $\alpha \leq \beta$ *tada* $\alpha \cdot \gamma \leq \beta \cdot \gamma$

Napomena 2.35. *Množenje ordinalnih brojeva općenito nije komutativno. Primjerice* $2 \cdot \omega =$ *(iz def.)* $= \sup\{2 \cdot n : n \in \omega\} = \omega$, *a po drugoj strani* $\omega \cdot 2 =$ *(iz def.)* $= \omega \cdot (1+1) = \omega + \omega \neq \omega$, *jer je očito* $\omega + \omega > \omega + 1 > \omega$.

Općenito ne vrijedi "desna" distributivnost, tj. ne mora vrijediti $(\alpha+\beta)\cdot\gamma = \alpha\cdot\gamma+\beta\cdot\gamma$. *Primjerice, vrijedi* $\omega = 2 \cdot \omega = (1+1) \cdot \omega \neq \omega + \omega$.

Definicija 2.36. *Primjenom teorema rekurzije slijedi da je s jednakostima koje slijede definirana jedinstvena skupovna operacija na* $On \times On$ *:*

$$\alpha^0 = 1$$

$$\alpha^{\beta+1} = \alpha^\beta \cdot \alpha$$

$$\alpha^\beta = \sup\{\alpha^\gamma : \gamma < \beta\}, \quad \textit{ako je } \beta \textit{ granični ordinalni broj.}$$

Upravo definiranu skupovnu operaciju nazivamo potenciranje ordinalnih brojeva.

U sljedećoj propoziciji ističemo osnovna svojstva potenciranja ordinalnih brojeva.

Propozicija 2.37. *(Svojstva potenciranja ordinalnih brojeva)*
Neka su α, β i γ proizvoljni ordinalni brojevi. Tada vrijedi:

a) $\alpha^\beta \cdot \alpha^\gamma = \alpha^{\beta+\gamma}$

b) $(\alpha^\beta)^\gamma = \alpha^{\beta\cdot\gamma}$

c) Ako je $\alpha > 1$ *i* $\beta < \gamma$ *tada je* $\alpha^\beta < \alpha^\gamma$

Napomena 2.38. *Općenito ne vrijedi $\alpha^\beta \cdot \gamma^\beta = (\alpha \cdot \gamma)^\beta$. To ilustriramo sljedećim primjerom:*

$$\begin{aligned}(\omega\cdot 2)^\omega &= \sup\{(\omega\cdot 2)^n : n\in\omega\}\\ &= \sup\{(\omega\cdot 2)\cdot\ldots\cdot(\omega\cdot 2) : n\in\omega\}\\ &= \sup\{\omega\cdot(2\cdot\omega)\cdot\ldots\cdot(2\cdot\omega)\cdot 2 : n\in\omega\}\\ &= \sup\{\omega^n\cdot 2 : n\in\omega\} \;=\; \omega^\omega\end{aligned}$$

$$\begin{aligned}\omega^\omega\cdot 2^\omega &= \sup\{\omega^\omega\cdot 2^n : n\in\omega\}\\ &= \omega^\omega\cdot\omega \;=\; \omega^{\omega+1}\end{aligned}$$

Alternativnu definiciju potenciranja ordinalnih brojeva možete pogledati u [31].

Istaknimo koje ordinalne brojeve sada znamo kada primijenimo upravo uvedene operacije:

$$0,\ 1,\ 2,\ \ldots,\ \omega,\ \omega+1,\ \omega+2,\ \ldots,\ \omega+\omega=\omega\cdot 2,\ \ldots,$$

$$\omega\cdot 2+1,\ \ldots,\omega\cdot 3,\ \ldots,\omega\cdot\omega=\omega^2,\ \ldots,\omega^3,\ \ldots,\omega^\omega,$$

$$\omega^\omega+1,\ \ldots,\omega^\omega\cdot 2,\ldots,\ \omega^{\omega^\omega},\ \ldots,\ \omega^{\omega^{\omega^\omega}},\ \ldots$$

Nije teško vidjeti da je svaki od navedenih ordinalnih brojeva prebrojiv skup. Primjerice, $\omega^\omega = \sup\{\omega^n : n\in\omega\} = \bigcup_{n\in\omega}\omega^n$, a pošto je svaki ordinalni broj oblika ω^n prebrojiv, tada je i ordinalni broj ω^ω prebrojiv. Najmanji ordinalni broj α za koji vrijedi $\omega^\alpha = \alpha$ označava se sa ϵ_0. Najmanji ordinalni broj koji je neprebrojiv skup označava se sa ω_1.

Zadaci

1. Dokažite propoziciju 2.25.
   Dokaz.
   a) Označimo $B = \bigcup_{\alpha \in A} \alpha$. Dokažimo da je skup B tranzitivan i dobro uređen skup. Neka su y i z skupovi takvi da vrijedi $y \in z \in B$. Iz definicije skupa B slijedi da postoji $\alpha \in A$ takav da je $z \in \alpha$. Pošto je α ordinalni broj, tj. posebno je tranzitivan, tada vrijedi $y \in \alpha$. Iz definicije skupa B slijedi $y \in B$.

   Neka su $x, y \in B$. Tada postoje $\alpha, \beta \in A$ takvi da je $x \in \alpha$ i $y \in \beta$. Iz propozicije 2.20. slijedi da vrijedi $\alpha \in \beta$ ili $\alpha = \beta$ ili $\beta \in \alpha$. Radi određenosti neka je $\alpha \in \beta$. Tada imamo $x \in \alpha \in \beta$. Pošto je β tranzitivan skup tada vrijedi $x \in \beta$. Sada iz $x, y \in \beta$ slijedi da su x i y usporedivi elementi u skupu B. Time smo dokazali da je B ordinalni broj.

   Dokažimo sada da je B supremum skupa A. Pošto očito za svaki $\alpha \in A$ vrijedi $\alpha \subseteq B$, te je B ordinalni broj, tada $\alpha \in B$ ili $\alpha \in B$. To znači da je B gornja međa skupa A. Pretpostavimo sada da je γ ordinalni broj koji je gornja međa skupa A. Tada za svaki $\alpha \in A$ vrijedi $\alpha \in \gamma$, a onda i $\alpha \subseteq \gamma$. Tada je očito $\bigcup_{\alpha \in A} \alpha \subseteq \gamma$, tj. $B \subseteq \gamma$. Ako je $B \neq \gamma$, te pošto je γ ordinalni broj, tada imamo $B \in \gamma$.

   b) Označimo $C = \bigcap_{\alpha \in A} \alpha$. Pretpostavimo da $y \in z \in C$. Tada za svaki $\alpha \in A$ vrijedi $y \in z \in \alpha$. Pošto je svaki $\alpha \in A$ tranzitivan skup tada vrijedi $y \in \alpha$, a onda imamo i $y \in C$. Neka su $x, y \in C$. Tada vrijedi $x, y \in \alpha$ za svaki $\alpha \in A$. Pošto je svaki $\alpha \in A$ linearno uređen skup tada vrijedi: $x \in y$ ili $x = y$ ili $y \in x$, tj. skup C je linearno uređen. Time smo dokazali da je skup C ordinalni broj. Očito je skup C infimum skupa A, jer ako je β donja međa skupa A tada vrijedi $\beta \in \alpha$, za svaki $\alpha \in A$, a onda imamo i $\beta \in C$.

2. Dokažite propoziciju 2.26.
   Dokaz. Lako je provjeriti da je $\alpha \cup \{\alpha\}$ tranzitivan i dobro uređen skup s relacijom $\in$. Dokažimo da je $\alpha \cup \{\alpha\}$ neposredni sljedbenik od α. Očito je $\alpha \in \alpha \cup \{\alpha\}$, tj. $\alpha < \alpha + 1$. Pretpostavimo da postoji ordinalni broj β tako da vrijedi $\alpha < \beta < \alpha + 1$. Tada iz definicije uređaja slijedi $\alpha \in \beta$ i $\beta \in \alpha \cup \{\alpha\}$. Iz ovog posljednjeg slijedi da je $\beta \in \alpha$ ili $\beta \in \{\alpha\}$. Ako bi vrijedilo $\beta \in \alpha$ tada iz $\alpha \in \beta$ slijedi $\alpha \in \alpha$, što je nemoguće zbog aksioma dobre utemeljenosti. To znači da bi moralo vrijediti $\beta \in \{\alpha\}$, tj. $\beta = \alpha$. No, ovo posljednje i $\alpha \in \beta$ opet vodi na $\alpha \in \alpha$.

   Dokažimo sada drugu tvrdnju. Neka vrijedi $\alpha < \beta$. Tada je $\alpha \in \beta$. Pretpostavimo li da je $\beta < \alpha + 1$ tada je $\beta \in \alpha \cup \{\alpha\}$. Iz ovog posljednjeg slijedi da su moguća sljedeća dva slučaja: $\beta \in \alpha$ ili $\alpha = \beta$. Oba slučaja vode na $\beta \in \beta$,

tj. na kontradikciju s aksiomom dobre utemeljenosti. Iz propozicije 2.20. slijedi da mora vrijediti $\alpha + 1 \leq \beta$.

3. Dokažite teorem 2.28.
   Dokaz. Pretpostavimo suprotno, tj. da postoji ordinalni broj α tako da formula $F(\alpha)$ nije dokaziva u teoriji ZF. Neka je $A = \{\beta \leq \alpha : \ \mathtt{ZF} \nvdash F(\beta).\}$ Pošto je A neprazan skup ordinalnih brojeva tada on ima najmanji element. Neka je γ najmanji element skupa A. No, za svaki $\beta < \gamma$ vrijedi $\mathtt{ZF} \vdash F(\beta)$, pa iz pretpostavke teorema slijedi da vrijedi i $\mathtt{ZF} \vdash F(\gamma)$. To je u kontradikciji s činjenicom da je $\gamma \in A$.

4. Neka je $\alpha \neq 0$ ordinalni broj. Dokažite da su sljedeće tvrdnje ekvivalentne:

   a) α je granični ordinalni broj;

   b) $\forall\beta(\beta < \alpha \Rightarrow \beta + 1 < \alpha)$;

   c) $\alpha = \sup\{\beta : \beta < \alpha\} \quad (= \bigcup_{\beta<\alpha} \beta)$.

5. Neka su $(A, <)$ i $(B, \prec)$ dobro uređeni skupovi. Definiramo **uređenu sumu** tih skupova, u oznaci $A + B$, kao uređeni par $(A \times \{0\} \cup B \times \{1\}, \lhd)$, pri čemu je $\lhd$ binarna relacija definirana sa:

$$(x, i) \lhd (y, j) \qquad \Leftrightarrow \qquad \begin{cases} 0 = i = j \ \text{ i } \ x < y \\ \qquad\quad \text{ili} \\ 1 = i = j \ \text{ i } \ x \prec y \\ \qquad\quad \text{ili} \\ i = 0 \ \text{ i } \ j = 1 \end{cases}$$

   Lako je provjeriti da je $A+B$ dobro uređeni skup. Neka je $o(A) = \alpha$ i $o(B) = \beta$. Dokažite da je tada $o(A + B) = \alpha + \beta$.

   Dokaz. Prvo dokazujemo dvije pomoćne tvrdnje.

   Tvrdnja 1. Neka su α i β ordinalni brojevi. Tada vrijedi:

$$\alpha + \beta = \alpha \cup \{\alpha + \gamma : \gamma < \beta\}.$$

   Dokaz tvrdnje 1. Traženju tvrdnju dokazujemo transfinitnom indukcijom po β. Ako je $\beta = 0$ tada je $\alpha + \beta = \alpha + 0 = \alpha$, te je $\alpha \cup \{\alpha + \gamma : \gamma < \beta\}$ $= \alpha \cup \{\alpha + \gamma : \gamma < 0\} = \alpha \cup \emptyset = \alpha$.
   Neka je $\beta = \gamma + 1$, te pretpostavimo da vrijedi $\alpha + \gamma = \alpha \cup \{\alpha + \delta : \delta < \gamma\}$. Tada imamo:

$$\begin{aligned}\alpha \cup \{\alpha+\delta : \delta<\beta\} &= \alpha \cup \{\alpha+\delta : \delta<\gamma\} \cup \{\alpha+\gamma\} \\ &= \text{(pretpostavka ind.)} \quad = (\alpha+\gamma) \cup \{\alpha+\gamma\} \\ &= (\alpha+\gamma)+1 \\ &= \text{(def. zbrajanja)} \quad = \alpha+(\gamma+1) = \alpha+\beta\end{aligned}$$

Pretpostavimo sada da je β granični ordinalni broj, te da za svaki $\gamma<\beta$ tvrdnja vrijedi. Pošto je β granični ordinalni broj, tada očito za svaki $\delta<\beta$ postoji ordinalni broj γ takav da $\delta<\gamma<\beta$. Tada redom imamo:

$$\begin{aligned}\alpha \cup \{\alpha+\delta : \delta<\beta\} &= \alpha \cup \bigcup_{\gamma<\beta}\{\alpha+\delta : \delta<\gamma\} \\ &= \bigcup_{\gamma<\beta}(\alpha \cup \{\alpha+\delta : \delta<\gamma\}) \\ &= \text{(pretpostavka ind.)} \quad = \bigcup_{\gamma<\beta}(\alpha+\gamma) \\ &= \sup\{\alpha+\gamma : \gamma<\beta\} = \alpha+\beta\end{aligned}$$

Time je tvrdnja 1 dokazana.

Tvrdnja 2. Neka su $\alpha,\beta,\gamma \in On$, te neka je $\gamma<\beta$. Tada vrijedi: $\alpha \leq \alpha+\gamma < \alpha+\beta$.

Dokaz tvrdnje 2. Znamo da za sve ordinalne brojeve α i β vrijedi:

$$\alpha \leq \beta \text{ ako i samo ako } \alpha \subseteq \beta \qquad (*)$$

Iz dokazane tvrdnje 1 imamo $\alpha+\gamma = \alpha \cup \{\alpha+x : x<\gamma\}$. No, desna strana je očito nadskup od α, pa iz $(*)$ slijedi $\alpha \leq \alpha+\gamma$.

Iz pretpostavke $\gamma<\beta$ i $(*)$ slijedi da vrijedi $\gamma \subset \beta$. Primjenom dokazane tvrdnje 1 slijedi $\alpha+\gamma \subset \alpha+\beta$. Time je tvrdnja 2 dokazana.

Sada dokazujemo tvrdnju zadatka. Neka su $f : A \to \alpha$ i $g : B \to \beta$ sličnosti. Definiramo funkciju $h : A\times\{0\} \cup B\times\{1\} \to \alpha+\beta$ sa $h(x,0) = f(x)$ i $h(y,1) = \alpha+g(y)$. Tada je $Rng(h) = Rng(f) \cup \{\alpha+g(y) : y \in B\} = \alpha \cup \{\alpha+\gamma : \gamma<\beta\}$ = (Tvrdnja 1) $= \alpha+\beta$. Time smo dokazali da je funkcija h surjekcija.

Dokažimo sada da funkcija h čuva uređaj. Neka vrijedi $(x,i) \lhd (y,j)$. Iz definicije uređaja na uređenoj sumi slijedi da imamo sljedeća tri slučaja:

a) $0 = i = j$ i $x<y$.
Tada je $h(x,0) = f(x) < f(y) = h(y,0)$, jer funkcija f čuva uređaj.

b) $1 = i = j$ i $x \prec y$.
Tada je $h(x,1) = \alpha+g(x)$ i $h(y,1) = \alpha+g(y)$. Iz dokazane tvrdnje 2, te činjenica $x \prec y$ i da je funkcija g sličnost, slijedi $\alpha+g(x) < \alpha+g(y)$.

c) $i = 0$ i $j = 1$.
Tada je $h(x, 0) = f(x)$ i $h(y, 1) = \alpha + g(y)$. Pošto je $f(x) \in \alpha$ tada je $f(x) < \alpha$. Iz dokazane tvrdnje 2 tada slijedi $f(x) < \alpha + g(y)$.

Očito je funkcija h injekcija.

6. Dokažite propoziciju 2.31.
Dokaz. Za ilustraciju dokazujemo tvrdnju b). Dokaz provodimo transfinitnom indukcijom po γ. Pretpostavimo da je γ ordinalni broj koji ima svojstvo da za svaki $\delta < \gamma$, te sve ordinalne brojeve α i β vrijedi $(\alpha + \beta) + \delta = \alpha + (\beta + \delta)$. Promotrimo prvo slučaj kada je ordinalni broj γ prve vrste, tj. postoji ordinalni broj δ tako da vrijedi $\gamma = \delta + 1$. Tada imamo:

$$\begin{aligned}
\alpha + (\beta + \gamma) &= \alpha + (\beta + (\delta + 1)) = \\
&= \text{(def. zbrajanja)} = \alpha + ((\beta + \delta) + 1) \\
&= \text{(def. zbrajanja)} = (\alpha + (\beta + \delta)) + 1 \\
&= \text{(pret. indukcije)} = ((\alpha + \beta) + \delta) + 1 \\
&= \text{(def. zbrajanja)} = (\alpha + \beta) + (\delta + 1) \\
&= (\alpha + \beta) + \gamma
\end{aligned}$$

Neka je sada γ granični ordinalni broj takav da za svaki ordinalni broj $x < \gamma$, te sve ordinalne brojeve α i β vrijedi tvrdnja. Tada redom imamo:

$$\begin{aligned}
\alpha + (\beta + \gamma) &= \alpha + (\beta + \sup\{x : x < \gamma\}) \\
&= \text{(def. zbrajanja)} = \alpha + \sup\{\beta + x : x < \gamma\} \\
&= \text{(def. zbrajanja)} = \sup\{\alpha + (\beta + x) : x < \gamma\} \\
&= \text{(pret. indukcije)} = \sup\{(\alpha + \beta) + x : x < \gamma\} \\
&= \text{(def. zbrajanja)} = (\alpha + \beta) + \sup\{x : x < \gamma\} \\
&= (\alpha + \beta) + \gamma
\end{aligned}$$

7. *(Teorem o oduzimanju)*
Neka su α i β ordinalni brojevi takvi da je $\beta \leq \alpha$. Dokažite da tada postoji jedinstveni ordinalni broj γ tako da vrijedi $\alpha = \beta + \gamma$.

Dokaz. Označimo $A = \{x : \beta + x \leq \alpha\}$. Neka je $\gamma = \sup A$. Tada je $\beta + \gamma \leq \alpha$. Pretpostavimo da je $\beta + \gamma < \alpha$. Tada iz propozicije 2.26. slijedi $(\beta + \gamma) + 1 \leq \alpha$, pa imamo $\alpha \geq (\beta + \gamma) + 1 = \beta + (\gamma + 1)$, iz čega slijedi da je $\gamma + 1 \in A$. No, to je nemoguće (jer bi tada imali $\gamma + 1 \leq \sup A = \gamma$). Jedinstvenost slijedi iz propozicije 2.31. c).

8. Neka su $(A, <)$ i $(B, <')$ dobro uređeni skupovi. Na Kartezijevom produktu $A \times B$ definiramo binarnu relaciju $\prec$ na sljedeći način:

$$(a_1, b_1) \prec (a_2, b_2) \qquad \Leftrightarrow \qquad \begin{cases} b_1 <' b_2 \\ \text{ili} \\ b_1 = b_2 \ \text{ i } \ a_1 < a_2 \end{cases}$$

Uređaj $\prec$ se naziva antileksikografski uređaj (vidi i primjer 1.62.). Lako je provjeriti da je $(A \times B, \prec)$ dobro uređeni skup. Dokažite da je tada $o(A \times B) = \alpha \cdot \beta$.

9. Dokažite propoziciju 2.34.

10. *(Teorem o dijeljenju s ostatkom)*
Neka su α i β ordinalni brojevi, te neka je $\beta > 0$. Tada postoje jedinstveni ordinalni brojevi δ i ρ takvi da je $\alpha = \beta \cdot \delta + \rho$, i $\rho < \beta$.
Dokaz. Ako je $\alpha < \beta$ tada možemo uzeti $\delta = 0$ i $\rho = \alpha$. Ako je $\alpha = \beta$ tada možemo uzeti da je $\delta = 1$ i $\rho = 0$. Pretpostavimo sada da je $\alpha > \beta$. Neka je $\delta = \sup\{x : \beta \cdot x \leq \alpha\}$. Tada je $\beta \cdot \delta \leq \alpha$. Iz teorema o oduzimanju, tj. zadatka 7, slijedi da postoji ordinalni broj ρ takav da je $\alpha = \beta \cdot \delta + \rho$.

Pretpostavimo da vrijedi $\beta \leq \rho$. Tada iz teorema o oduzimanju, tj. zadatka 7, slijedi da postoji ordinalni broj γ takav da je $\rho = \beta + \gamma$. Sada iz toga slijedi $\alpha = \beta \cdot \delta + \rho = \beta \cdot \delta + (\beta + \gamma) = \beta \cdot (\delta + 1) + \gamma$, pa δ nije supremum skupa $\{x : \beta \cdot x \leq \alpha\}$, što je suprotno pretpostavci. To znači da mora vrijediti $\rho < \beta$.

Preostalo je dokazati jedinstvenost. Neka je $\alpha = \beta \cdot \delta + \rho$, gdje je $\rho < \beta$. Pretpostavimo da δ nije supremum skupa $\{x : \beta \cdot x \leq \alpha\}$. Tada je očito $\alpha > \beta \cdot \delta$, a onda je $\alpha \geq \beta \cdot (\delta + 1)$. Sada imamo:

$$\alpha \geq \beta \cdot (\delta + 1) = \beta \cdot \delta + \beta > \beta \cdot \delta + \rho = \alpha,$$

što je nemoguće. Time je dokazana jedinstvenost ordinalnog broja δ. Jedinstvenost ordinalnog broja ρ slijedi iz propozicije 2.31.

11. Dokažite propoziciju 2.37.

12. *(Teorem o logaritamskom algoritmu)*
Neka su $\alpha \neq 0$ i $\beta > 1$ ordinalni brojevi. Dokažite da postoje jedinstveni ordinalni brojevi γ, δ i ρ takvi da je $0 < \delta < \beta$ i $\rho < \beta^\gamma$, te vrijedi $\alpha = \beta^\gamma \delta + \rho$.
Dokaz. Neka je $\gamma = \sup\{x : \beta^x \leq \alpha\}$. Primjenom teorema o dijeljenju s

ostatkom, tj. zadatka 10, slijedi da postoje jedinstveni ordinalni brojevi δ i ρ, takvi da je $\rho < \beta^\gamma$ i $\alpha = \beta^\gamma\delta + \rho$.

Dokažimo da vrijedi $0 < \delta < \beta$. Ako bi vrijedilo $\delta = 0$ tada bi imali $\rho = \alpha \geq \beta^\gamma > \rho$, što je kontradikcija. Pretpostavimo da je $\delta \geq \beta$. Tada imamo:

$$\alpha < \beta^{\gamma+1} = \beta^\gamma\beta \leq \beta^\gamma\delta \leq \beta^\gamma\delta + \rho = \alpha,$$

što je kontradikcija.

Dokažimo sada jedinstvenost. Neka vrijedi $\alpha = \beta^\gamma\delta + \rho$, i pretpostavimo da γ nije supremum skupa $\{x : \beta^x \leq \alpha\}$. Tada imamo:

$$\alpha \geq \beta^{\gamma+1} = \beta^\gamma\beta \geq \beta^\gamma(\delta+1) = \beta^\gamma\delta + \beta^\gamma > \beta^\gamma\delta + \rho = \alpha,$$

što je kontradikcija. Sada jedinstvenost ordinalnih brojeva δ i ρ slijedi iz zadatka 10.

13. *(Teorem o normalnoj formi ordinalnih brojeva)*[2]
Neka su α i β ordinalni brojevi i $\beta > 1$. Dokažite da postoji jedinstveni prirodan broj n i konačni nizovi ordinalnih brojeva $\gamma_0, \ldots, \gamma_n$ i $\delta_0, \ldots, \delta_n$ tako da vrijedi:

$$\gamma_0 > \gamma_1 > \ldots > \gamma_n,$$

$$0 < \delta_i < \beta, \quad \text{za svaki } i \leq n,$$

$$\alpha = \beta^{\gamma_0}\delta_0 + \beta^{\gamma_1}\delta_1 + \ldots + \beta^{\gamma_n}\delta_n$$

Dokaz. Primjenom teorema o logaritamskom algoritmu slijedi da postoje jedinstveni ordinalni brojevi γ_0, δ_0 i ρ_0 tako da vrijedi $0 < \delta_0 < \beta$, $\rho < \beta^{\gamma_0}$ i

$$\alpha = \beta^{\gamma_0}\delta_0 + \rho_0.$$

Ako je $\rho_0 = 0$ tada je teorem dokazan. Ako pak je $\rho_0 > 0$ tada na njega primjenimo teorem o logaritamskom algoritmu.

Važno je primijetiti da taj postupak mora stati u konačno mnogo koraka. Inače bi postojao beskonačan niz ordinalnih brojeva (γ_k) tako da za svaki k vrijedi $\gamma_k > \gamma_{k+1}$. To znači da taj niz ne bi imao najmanji element. No, to je nemoguće

[2] Točan naziv teorema je teorem o normalnoj formi po bazi β. Ako je $\beta = 2$ tada govorimo o diadskoj normalnoj formi, a ako pak je $\beta = \omega$ tada govorimo o Cantorovoj normalnoj formi. Dakle, za svaki ordinalni broj α postoji jedinstveni prirodan broj n i konačni nizovi ordinalnih brojeva $\gamma_0 > \gamma_1 > \ldots \gamma_n$ i $m_0, \ldots, m_n$, gdje su svi m_i konačni ordinalni brojevi, te vrijedi

$$\alpha = \omega^{\gamma_0}m_0 + \omega^{\gamma_1}m_1 + \ldots + \omega^{\gamma_n}m_n.$$

zbog aksioma dobre utemeljenosti. Jedinstvenost slijedi iz teorema o logaritamskom algoritmu.

2.4 Kardinalni brojevi

Podsjetimo se da smo na samom početku u naivnoj teoriji skupova spominjali pojam kardinalnosti (kao oznaku svojstva), tj. rekli smo da skupovi A i B imaju istu kardinalnost ako su ekvipotentni. No, nismo definirali što je zapravo kardinalni broj. Sada to činimo.

Definicija 2.39. Kardinalni broj λ *je ordinalni broj koji ima svojstvo da niti za jedan* $\alpha < \lambda$ *ne postoji bijekcija između* λ *i* α.

U sljedećem teoremu navodimo primjere kardinalnih brojeva.

Teorem 2.40. *Vrijede sljedeće tvrdnje:*

a) Svaki konačni ordinalni broj je kardinalni broj;

b) Skup ω *je kardinalni broj;*

c) Svaki beskonačni kardinalni broj je granični ordinalni broj.

Primijetimo da svaki granični ordinalni broj nije kardinalni broj. Npr. $\omega + \omega$ nije kardinalni broj.

Kako bismo mogli definirati kardinalni broj proizvoljnog skupa sada ćemo iskazati Zermelov teorem o dobrom uređaju. Taj teorem je ekvivalentan s aksiomom izbora. Aksiom izbora je glavna tema sljedeće točke.

Teorem 2.41. *(Zermelov teorem o dobrom uređaju)*
Svaki skup se može dobro urediti. Odnosno, ako je A *skup tada postoji binarna relacija* $R \subseteq A \times A$ *tako da je uređeni par* (A, R) *dobro uređeni skup.*

Neka je A proizvoljan skup. Iz Zermelovog teorema o dobrom uređaju slijedi da na skupu A postoji dobar uređaj. Iz teorema enumeracije, tj. teorema 2.22., tada slijedi da postoji ordinalni broj α takav da vrijedi $A \simeq \alpha$. To znači da je klasa $\{\beta : \beta \in On \text{ i } A \sim \beta\}$ neprazna. Bili smo dokazali da svaka klasa ordinalnih brojeva ima najmanji element. Ova razmatranja opravdavaju sljedeću definiciju.

Definicija 2.42. *Kardinalni broj proizvoljnog skupa* A *definiramo kao najmanji ordinalni broj* λ *za koji vrijedi* $A \sim \lambda$. *Kardinalni broj skupa* A *označavamo sa* $k(A)$.

Uočite da je za svaki skup A ordinalni broj $k(A)$ zapravo kardinalni broj. Ako je λ kardinalni broj tada je očito $k(\lambda) = \lambda$. Očito je $k(\omega) = \omega$, te $k(\omega + 1) = \omega$ i $k(\omega^\omega) = \omega$.

Iz definicije očito slijedi da ekvipotentni skupovi imaju jednak kardinalni broj. Ta činjenica i sljedeća definicija operacija na kardinalnim brojevima omogućavaju nam da ovdje možemo samo istaknuti svojstva operacija na kardinalnim brojevima bez da ih moramo dokazivati. Dokazi tih svojstava bili bi sasvim isti kao u naivnoj teoriji skupova.

Definicija 2.43. *Neka su λ i μ kardinalni brojevi. Tada definiramo:*

a) $\lambda + \mu = k(\lambda \times \{0\} \cup \mu \times \{1\})$

b) $\lambda \cdot \mu = k(\lambda \times \mu)$

c) $\lambda^\mu = k(\{f |\ f : \mu \to \lambda\})$

Napomena 2.44. *Važno je spomenuti da operacije zbrajanja, množenja i potenciranja za ordinalne i kardinalne brojeve isto označavamo. No, to nisu iste operacije. Npr. ako ω i 1 zbrajamo kao ordinalne brojeve tada je to $\omega + 1$ (što je različito od ω). No, ako ω i 1 zbrajamo kao kardinalne brojeve tada je to ω (jer je $\omega \times \{0\} \cup 1 \times \{1\} \sim \omega$).*

Sada samo ističemo svojstva operacija na kardinalnim brojevima. Dokazi tih svojstava, kao što smo već bili napomenuli, su sasvim isti kao u naivnoj teoriji, pa ih ovdje nećemo ponavljati.

Teorem 2.45. *Neka su λ, μ i ν kardinalni brojevi. Tada vrijedi:*

a) $\lambda + (\mu + \nu) = (\lambda + \mu) + \nu$

b) $\lambda + \mu = \mu + \lambda$

c) $\lambda \cdot (\mu \cdot \nu) = (\lambda \cdot \mu) \cdot \nu$

d) $\lambda \cdot \mu = \mu \cdot \lambda$

e) $\lambda \cdot (\mu + \nu) = \lambda \cdot \mu + \lambda \cdot \nu$

f) $\lambda^\nu \cdot \mu^\nu = (\lambda \cdot \mu)^\nu$

g) $\lambda^{\mu+\nu} = \lambda^\mu \cdot \lambda^\nu$

h) $(\lambda^\mu)^\nu = \lambda^{\mu \cdot \nu}$

Teorem 2.46. *(Cantorov osnovni teorem)*
Za svaki kardinalni broj λ vrijedi $\lambda < 2^\lambda$.
(Uređaj je naslijeđen s ordinalnih brojeva).

Primijetimo da je to u stvari tvrdnja Cantorovog osnovnog teorema teorije skupova, tj. teorema 1.57.

Teorem 2.47. *Ako su λ i μ kardinalni brojevi takvi da vrijedi $\lambda \leq \mu$ i $\mu \leq \lambda$ tada imamo $\lambda = \mu$.*

Uočimo da je to je zapravo Cantor, Schröder, Bernsteinov teorem, tj. teorem 1.40.

Lema 2.48. *Za svaki kardinalni broj λ postoji kardinalni broj koji je neposredni sljedbenik od λ. Neposredni sljedbenik od λ označavamo sa λ^+.*

Dokaz. Iz teorema 2.46. slijedi da je klasa $\{\mu : \mu$ je kardinalni broj i $\lambda < \mu\}$ neprazna. To je posebno klasa ordinalnih brojeva, pa sadrži najmanji element.Q.E.D.

Lema 2.49. *Ako je S skup kardinalnih brojeva tada je $\cup S$ također kardinalni broj.*

Dokaz. Iz propozicije 2.25. znamo da je $\cup S$ ordinalni broj. Pretpostavimo da je $k(\cup S) < \cup S$. Pošto je relacija uređaja po definiciji zapravo relacija $\in$ tada postoji $\gamma \in S$ takav da je $k(\cup S) < \gamma$. No, očito je $\gamma \subseteq \cup S$, pa imamo $\gamma = k(\gamma) \leq k(\cup S) < \gamma$, što je kontradikcija. Q.E.D.

Primjenom prethodne leme slijedi da za svaki skup S kardinalnih brojeva postoji kardinalni broj koji je supremum skupa S. Supremum skupa S označavamo sa $\sup S$.

Propozicija 2.50. *Klasa svih kardinalnih brojeva Cn je prava klasa.*

Dokaz. Pretpostavimo da je klasa Cn skup. Tada iz leme 2.49. znamo da je $\sup Cn \in Cn$. Iz leme 2.48. slijedi da postoji $\mu \in Cn$ takav da je $\sup\ Cn < \mu$, što je kontradikcija. Q.E.D.

Definicija 2.51. *Sa $\aleph$ označavamo skupovnu operaciju s klase svih ordinalnih brojeva On u klasu svih beskonačnih kardinalnih brojeva koja je pomoću rekurzije definirana ovako:*

$$\aleph_0 = \omega$$

$$\aleph_{\beta+1} = \aleph_\beta^+$$

$$\aleph_\alpha = \sup\{\aleph_\beta : \beta < \alpha\}, \quad \textit{ako je } \alpha \textit{ graničnI ordinalni broj.}$$

Uočite da nam leme 2.48. i 2.49., te teorem rekurzije, garantiraju da je prethodna definicija dobra.

Kada želimo istaknuti da ordinalni broj ω promatramo kao kardinalni broj tada umjesto ω pišemo $\aleph_0$. Analogno za ostale kardinalne brojeve. Ta razlika u notaciji nam je posebno važna kada želimo naglasiti radi li se o ordinalnoj ili kardinalnoj aritmetici. Prilikom razmatranja aksioma izbora dokazat ćemo da su zbrajanje i množenje kardinalnih brojeva trivijalne operacije, tj. da vrijedi: *ako su α i β ordinalni brojevi takvi da je $\alpha \leq \beta$, tada $\aleph_\alpha + \aleph_\beta = \aleph_\alpha \cdot \aleph_\beta = \aleph_\beta$.*

Sada Cantorovu hipotezu kontinuuma možemo zapisati i ovako: $2^{\aleph_0} = \aleph_1$, odnosno opća Cantorova hipoteza glasi: za svaki ordinalni broj α vrijedi $2^{\aleph_\alpha} = \aleph_{\alpha+1}$.

Vrlo se malo zna o kardinalnim brojevima $2^{\aleph_\alpha}$ i $\aleph_\alpha^{\aleph_\beta}$. O aritmetici kardinalnih brojeva možete više naći u [15], [18], [19], [28] i [34].

Zadaci

1. Dokažite teorem 2.40.
2. Pokažite primjerom da općenito ne vrijedi da $\lambda + \mu = \lambda + \nu$ povlači $\mu = \nu$.
3. Pokažite primjerom da općenito ne vrijedi da $\lambda \cdot \mu = \lambda \cdot \nu$ povlači $\mu = \nu$.
4. Neka su λ, μ i ν kardinalni brojevi. Dokažite da tada vrijedi:

   a) ako je $\lambda \leq \mu$ tada je $\lambda + \nu \leq \mu + \nu$

   b) ako je $\lambda \leq \mu$ tada je $\lambda \cdot \nu \leq \mu \cdot \nu$

   c) ako je $\lambda \leq \mu$ tada je $\lambda^\nu \leq \mu^\nu$

   d) ako je $\lambda \leq \mu$ i $\nu \neq 0$ tada je $\nu^\lambda \leq \nu^\mu$

5. Neka je $\mathcal{F} = (f_i : i \in I)$ familija međusobno različitih analitičkih funkcija na skupu $\mathbb{C}$. Kažemo da familija $\mathcal{F}$ ima svojstvo (P_0) ako je za svaki $z \in \mathbb{C}$ skup $\{f_i(z) : i \in I\}$ prebrojiv. Dokažite da vrijedi:

   a) ako je $c > \aleph_1$ tada je svaka familija $\mathcal{F}$ koja ima svojstvo (P_0) prebrojiva;

   b) ako je $c = \aleph_1$ tada postoji familija $\mathcal{F}$ koja ima svojstvo (P_0) i kardinaliteta je c.

   (Za dokaz vidite [2]).

2.5 Aksiom izbora

Na samom početku ove skripte bili smo naveli aksiom izbora. Prisjetimo se da smo aksiom izbora koristili prilikom dokaza da svaki beskonačan skup sadrži prebrojiv podskup, zatim da je prebrojiva unija prebrojivih skupova također prebrojiv skup, te za definiciju kardinalnog broja proizvoljnog skupa. Zatim, bili smo naveli **aksiom prebrojivog izbora**:

> *ako je* $\{A_0, A_1, A_2, \ldots\}$ *prebrojiv skup nepraznih skupova koji su u parovima disjunktni tada postoji niz* (a_n) *takav da je za svaki* $n \in \mathbb{N}$ *ispunjeno da je* $a_n \in A_n$.

Taj aksiom se često koristi u matematičkoj analizi. Kao malo ilustraciju primjene aksioma prebrojivog izbora u sljedećem primjeru dokazujemo da je mjera prebrojive unije skupova, čija je mjera nula, također nula.

Primjer 2.52. *Neka je* $\{A_n : n \in \mathbb{N}\}$ *prebrojiv skup čiji su elementi skupovi mjere nula. Neka je* $\epsilon > 0$ *proizvoljan. Za svaki* $n \in \mathbb{N}$ *neka je* O_n *neki otvoreni nadskup od* A_n *takav da je* $\mu(O_n) \leq \epsilon/2^{n+1}$ *(tu koristimo aksiom prebrojivog izbora). Tada je* $\mu(\bigcup_{n\in\mathbb{N}} A_n) \leq \sum_{n\in N} \mu(O_n) \leq \sum_{n\in\mathbb{N}} \epsilon/2^{n+1} = \epsilon$. *Time smo dokazali da je* $\mu(\bigcup_{n\in\mathbb{N}} A_n) < \epsilon$, *za svaki* $\epsilon > 0$. *Tada je očito* $\mu(\bigcup_{n\in\mathbb{N}} A_n) = 0$.

Pomoću aksioma izbora se dokazuju primjerice sljedeće činjenice:

1. Svaki vektorski prostor ima algebarsku bazu.
2. Svako polje ima algebarski zatvoreno proširenje.
3. Teorem Tihonova: Produkt kompaktnih topoloških prostora je kompaktan.
4. Teorem o ultrafiltru: Svaki pravi filtar je sadržan u nekom ultrafiltru.
5. Ekvivalentnost Heineove i Cauchyeve definicije neprekidnosti funkcije.

Hahn–Banachov teorem iz funkcionalne analize, teorem kompaktnosti i Löwenheim–Skolemov teorem u matematičkoj logici ekvivalentni su aksiomu izbora. Aksiom izbora je jedan od najviše razmatranih aksioma u matematici. Možda je više diskusije izazvao samo Euklidov peti postulat o paralelama. Aksiomi teorije skupova omogućavaju zasnivanje matematike na isti način kako su Euklidovi postulati omogućili zasnivanje Euklidove geometrije, te su pitanja vezana uz aksiom izbora ista kao i pitanja vezana uz Euklidov peti postulat:

1. Može li se izvesti iz ostalih aksioma?
2. Je li konzistentan s drugim aksiomima?
3. Moramo li ga prihvatiti kao aksiom teorije?

Zašto je aksiom izbora tako (bio) sporan? Koje mu je sada mjesto u matematičkoj logici, odnosno matematici? Na ova pitanja pokušat ćemo odgovoriti u razmatranjima koje slijede.

Ako su $A_1, \ldots, A_n$ konačni skupovi tada iz teorema o uzastopnom prebrojavanju slijedi da je skup $A_1 \times \ldots \times A_n$ također konačan, odnosno da postoji samo konačno mnogo "izbora" $(a_1, \ldots, a_n)$ takvih da je $a_i \in A_i$. To znači da nam za konačne familije konačnih skupova ne treba aksiom izbora.

Glavna kritika aksioma izbora je vezana uz njegovu nekonstruktivnost, tj. aksiom izbora tvrdi egzistenciju nekog skupa, ali ne daje nikakav algoritam kako taj skup konstruirati. Zgodan primjer koji lijepo ilustrira nekonstruktivnost aksioma izbora je Vitalijev skup.

Primjer 2.53. *(Vitalijev skup)*
Na zatvorenom segmentu $[0,1]$ *definiramo binarnu relaciju* $\sim$ *na sljedeći način:* $x \sim y$ *ako i samo ako* $x-y \in \mathbb{Q}$. *Lako je provjeriti da je* $\sim$ *relacija ekvivalencije. Kvocijentni skup* $[0,1]/\sim$ *je familija u parovima disjunktnih skupova. Iz aksioma izbora slijedi da postoji skup koji sadrži točno po jedan element iz svake klase ekvivalencije. Taj skup se naziva Vitalijev skup. Nemamo nikakvu predodžbu koji je to skup. Ne znamo čak niti jedan njegov element.*

Cilj nam je navesti neke ekvivalentne tvrdnje aksiomu izbora. Sada prvo ponavljamo izreku aksioma izbora koju ćemo koristiti u daljnjim razmatranjima.

Aksiom izbora [AC]
Neka je $(A_i : i \in I)$ *neprazna familija u parovima disjunktnih nepraznih skupova. Tada postoji skup* B *takav da je* $B \cap A_i$ *jednočlan skup za svaki* $i \in I$.
Skup B *se naziva* **izborni skup** *za familiju* $(A_i : i \in I)$.

Pretpostavka da su članovi familije u parovima disjunktni je nužna. Promotrimo familiju skupova $\{\{1\},\ \{2\},\ \{1,2\}\}$ čiji članovi nisu u parovima disjunktni. Očito ne postoji izborni skup za tu familiju.

Napomena 2.54. *Ako je* $A = \{0,1\}$ *tada je* $A^\omega \neq \emptyset$, *jer sadrži primjerice nul–niz. Želimo istaknuti da bez aksioma izbora ne možemo dokazati da je za proizvoljnu prebrojivu familiju* $(A_n : n \in \mathbb{N})$ *dvočlanih skupova Kartezijev produkt* $\prod A_n$ *neprazan. U prvi tren čini se da je sljedeće zaključivanje pravilno: pošto je svaki skup* A_n *ekvipotentan sa* $\{0,1\}$ *tada je skup* A^ω *ekvipotentan sa* $\prod A_n$. *Greška u ovom zaključivanju je sljedeća: za konstrukciju takve bijekcije za svaki* n *moramo izabrati jednu od dvije bijekcije između* A_n *i* $\{0,1\}$.

Russell je kao ilustraciju primjene aksioma izbora naveo prebrojive familije parova cipela i prebrojive familije parova čarapa. Za prvu familiju imamo egzistenciju izbornog skupa bez primjene aksioma izbora, dok nam je za izbor prebrojivo čarapa, pri čemu iz svakog para biramo točno jednu čarapu, potreban aksiom izbora.

Teorem 2.55. *Sljedeće tvrdnje su ekvivalentne sa [AC]:*

a) **Zornova lema**. *Neka je* $(A, <)$ *parcijalno uređen skup koji ima svojstvo da svaki neprazni lanac iz* A *ima gornju među u* A. *Tada* $(A, <)$ *ima barem jedan maksimalni element.*

b) **Hausdorffov princip maksimalnosti**. *Neka je* $(A, <)$ *parcijalno uređen skup. Tada za svaki lanac* L *od* A *postoji maksimalni lanac koji ga sadrži.*

c) **Zermelov teorem o dobrom uređaju**. *Svaki skup se može dobro urediti, tj. za svaki skup* A *postoji relacija* $R \subseteq A \times A$ *takva da je* (A, R) *dobro uređen skup.*

d) **Hartogsov teorem**. *Ako su A i B proizvoljni skupovi tada vrijedi $k(A) \leq k(B)$ ili $k(B) \leq k(A)$.*

e) **Teorem Tarskog**. *Ako je λ beskonačni kardinalni broj tada je $\lambda^2 = \lambda$.*

Dokaz prethodnog teorema je dan kroz rješenja niza zadatka koji su na kraju ove točke.

Korolar 2.56. *Za sve kardinalne brojeve $\lambda \neq 0$ i $\mu \neq 0$ od kojih je barem jedan beskonačan vrijedi:*

$$\lambda + \mu = \lambda \cdot \mu = \max\{\lambda, \mu\}.$$

Neke posljedice aksioma izbora su zbunjujuće, a neke čak paradoksalne. Iz aksioma izbora slijedi Zermelov teorem o dobrom uređaju, tj. da se svaki skup može dobro urediti. Iz toga posebno slijedi da se može dobro urediti skup realnih brojeva $\mathbb{R}$. Znate li neki dobar uređaj na skupu $\mathbb{R}$? Jedna paradoksalna posljedica aksioma izbora je sljedeći teorem.

Teorem 2.57. *(Banach, Tarskijev teorem)*
Neka su k i K kugle u $\mathbb{R}^3$. Tada postoji $n \in \mathbb{N}$ i particija $k_1, \ldots, k_n$ od k, te postoji particija $K_1, \ldots, K_n$ od K, tako da je za svaki $i = 1, \ldots, n$ skup k_i izometričan sa K_i.

Primijetite da skupovi k_i i K_i nisu izmjerivi. Dokaz Banach, Tarksijevog teorema možete vidjeti u [40] ili [5].

Napomena 2.58. *K. Gödel je 1939. godine dokazao da ako pretpostavimo da je teorija ZF bez aksioma izbora konzistentna tada je i teorija ZF s aksiomom izbora konzistentna. P. Cohen je 1963. godine dokazao da se u teoriji ZF bez aksioma izbora ne može dokazati [AC] (vidi [11], [21] i [6]).*

Zadaci

1. Možemo li u teoriji skupova ZF bez aksioma izbora izabrati (tj. dokazati da postoji) jedan element u:

   (a) nekom konačnom skupu? (DA)

   (b) nekom beskonačnom skupu? (DA)

   (c) svakom članu beskonačne familije jednočlanih skupova? (DA)

   (d) svakom članu beskonačne familije čiji svaki skup je konačan? (NE)

   (e) svakom članu konačne familije skupova čiji svaki skup je beskonačan? (DA)

(f) svakom članu beskonačne familije čiji svaki skup sadrži konačno mnogo realnih brojeva? (DA)

O gornjim tvrdnjama vidite [39].

2. Dokažite da su sljedeće tvrdnje ekvivalentne s $[AC]$:

$[AC]_1$ Neka je $(A_i : i \in I)$ neprazna familija nepraznih skupova.
Tada postoji $f : I \to \bigcup_{i\in I} A_i$ takva da je $f(i) \in A_i$, za svaki $i \in I$.
Funkcija f se naziva **funkcija izbora**.

$[AC]_2$ Neka je $A \neq \emptyset$. Tada postoji funkcija $f : \mathcal{P}(A) \setminus \{\emptyset\} \to A$
takva da je $f(B) \in B$, za svaki $\emptyset \neq B \subseteq A$.

$[AC]_3$ Neka je $A \neq \emptyset$ i $\mathcal{A} = \{A_i : i \in I\}$ neka particija skupa A.
Tada postoji funkcija $g : \mathcal{A} \to A$ takav da je $g(A_i) \in A_i$, za svaki $i \in I$.

$[R]$ **Russellov multiplikativni aksiom**
Neka je $(A_i : i \in I)$ familija skupova. Ako je $\prod_{i\in I} A_i$ prazan skup,
tada postoji $i \in I$ takav da je $A_i = \emptyset$.

Dokaz. Redom ćemo dokazati sljedeće implikacije:
$[AC] \Rightarrow [AC]_1 \Rightarrow [AC]_2 \Rightarrow [AC]_3 \Rightarrow [R] \Rightarrow [AC]$.

$\underline{[AC] \Rightarrow [AC]_1}$ Neka je $(A_i : i \in I)$ neprazna familija nepraznih skupova. Za svaki $i \in I$ definiramo $B_i = A_i \times \{i\}$. Uočimo da je za svaki $i \in I$ skup $B_i \neq \emptyset$, te je $B_i \cap B_j = \emptyset$, za sve $i \neq j$. Primjenom [AC] na familiju $(B_i : i \in I)$ slijedi da postoji skup B takav da je $B \cap B_i$ jednočlan skup za svaki $i \in I$. Neka je $a_i \in \bigcup_{i\in I} A_i$ takav da je $B \cap B_i = \{(a_i, i)\}$. Definiramo funkciju $f : I \to \bigcup_{i\in I} A_i$ sa $f(i) = a_i$, za svaki i. Očito je $f(i) \in A_i$, za svaki $i \in I$.

$\underline{[AC]_1 \Rightarrow [AC]_2}$ Neka je A neprazan skup. Tada je $\{B : B \in \mathcal{P}(A) \setminus \{\emptyset\}\}$ neprazna familija nepraznih skupova. Primjenom $[AC]_1$ slijedi da postoji funkcija $f : \mathcal{P}(A) \setminus \{\emptyset\} \to \bigcup_{B\in\mathcal{P}(A)\setminus\{\emptyset\}} B$, tako da vrijedi $f(B) \in B$, za svaki $\emptyset \neq B \subseteq A$.

$\underline{[AC]_2 \Rightarrow [AC]_3}$ Neka je $A \neq \emptyset$ i $\mathcal{A} = \{A_i : i \in I\}$ neka particija skupa A. Iz $[AC]_2$ slijedi da postoji funkcija $f : \mathcal{P}(A) \setminus \{\emptyset\} \to A$ takva da vrijedi $f(B) \in B$, za svaki $\emptyset \neq B \subseteq A$. Pošto za svaki $i \in I$ vrijedi $A_i \in \mathcal{P}(A) \setminus \{\emptyset\}$, tada za svaki $i \in I$ vrijedi $f(A_i) \in A_i$. To znači da za restrikciju funkcije f na $\mathcal{A}$ vrijedi traženo svojstvo.

$\underline{[AC]_3 \Rightarrow [R]}$ Neka je $(A_i : i \in I)$ neka familija skupova. Pretpostavimo da je za

svaki $i \in I$ skup A_i neprazan. Za svaki $i \in I$ definiramo $B_i = A_i \times \{i\}$. Tada je $\mathcal{B} = (B_i : i \in I)$ particija skupa $B = \bigcup_{i \in I} B_i$. Iz $[AC]_3$ slijedi da postoji funkcija $g : \mathcal{B} \to B$ tako da za svaki $i \in I$ vrijedi $g(B_i) \in B_i$. To znači da za svaki $i \in I$ postoji $a_i \in A_i$ tako da je $g(B_i) = (a_i, i)$. Sada definiramo $f : I \to \bigcup_{i \in I} A_i$ sa $f(i) = a_i$. Iz toga slijedi da je $\prod_{i \in I} A_i \neq \emptyset$.

$[R] \Rightarrow [AC]$ Neka je $(A_i : i \in I)$ neprazna familija nepraznih skupova koji su u parovima disjuktni. Iz Russellovog multiplikativnog aksioma slijedi da je $\prod_{i \in I} A_i \neq \emptyset$, tj. postoji $f : I \to \bigcup_{i \in I} A_i$ takva da za svaki $i \in I$ vrijedi $f(i) \in A_i$. Sada traženi izborni skup definiramo s $B = \{f(i) : i \in I\}$.

3. Dokažite da Zornova lema povlači Hausdorffov princip maksimalnosti.
   Dokaz. Neka je $(A, <)$ parcijalno uređen skup i $L \subseteq A$ neki lanac. Neka je $\mathcal{L}$ skup svih lanaca L' od A za koje vrijedi da je $L \subseteq L'$. Očito je $(\mathcal{L}, \subset)$ parcijalno uređen skup koji zadovoljava uvjete Zornove leme (ako je $\mathcal{A}$ neki lanac od $\mathcal{L}$ tada je $\cup\mathcal{A}$ lanac koji je jedna gornja međa za $\mathcal{A}$). Iz Zornove leme slijedi da parcijalno uređen skup $(\mathcal{L}, \subset)$ sadrži maksimalni element.

4. Dokažite da Zermelov teorem povlači Hartogsov terome.
   Dokaz. Neka su A i B dva proizvoljna skupa. Iz Zermelovog teorema slijedi da postoje binarne relacije $R \subseteq A \times A$ i $Q \subseteq B \times B$ takve da su skupovi (A, R) i (B, Q) dobro uređeni. Iz teorema 1.89. slijedi da je ispunjeno barem jedno od: A je sličan s B, A je sličan nekom početnom komadu od B, ili obratno. Tada posebno slijedi da postoji injekcija iz A u B, ili obratno.

5. Dokažite da Zermelov teorem povlači aksiom izbora.
   Dokaz. Neka je $(A_i : i \in I)$ neprazna familija nepraznih skupova koji su u parovima disjunktni. Iz Zermelovog teorema slijedi da se skup $\bigcup_{i \in I} A_i$ može dobro urediti. Za svaki $i \in I$ označimo s a_i najmanji element od A_i. Tada je $B = \{a_i : i \in I\}$ jedan izborni skup za danu familiju.

6. Dokažite da Zornova lema povlači Zermelov teorem.
   Dokaz. Neka je A proizvoljan skup. Označimo s $\mathcal{D}$ skup svih podskupova od A koji se mogu dobro urediti, tj.
   $\mathcal{D} = \{X \subseteq A :$ postoji $R \subseteq X \times X$ tako da je (X, R) dobro uređen skup$\}$.

   Za $X \subseteq A$ kažemo da je inicijalni segment ako za svaki $y \in A$ i $x \in X$ iz činjenice $y < x$ slijedi $y \in X$. Lako je vidjeti da je svaki inicijalni segment od A ili početni komad od A ili pak je jednak A. Inicijalni segment od A koji je različit od A nazivamo pravi inicijalni segment. Na skupu $\mathcal{D}$ definiramo binarnu relaciju $\prec$ ovako:
   $(X, R_X) \prec (Y, R_Y) \Leftrightarrow R_X \subset R_Y$ i X je pravi inicijalni segment od Y.

Očito je $(\mathcal{D}, \prec)$ parcijalno uređen skup. Želimo dokazati da $(\mathcal{D}, \prec)$ ispunjava uvjet Zornove leme. U tu svrhu izaberimo $\{(X_i, R_i) : i \in I\}$ proizvoljan lanac u $\mathcal{D}$. Tvrdimo da je $\mathcal{U} = (\bigcup_{i\in I} X_i, \bigcup_{i\in I} R_i)$ element od $\mathcal{D}$. Očito je $\mathcal{U}$ linearno uređen skup.

Dokažimo da je $\mathcal{U}$ dobro uređen skup. Neka je Y proizvoljan neprazan podskup od $\bigcup_{i\in I} X_i$. Tada postoji $i_0 \in I$ takav da je $Y \cap X_{i_0} \neq \emptyset$. Pošto je (X_{i_0}, R_{i_0}) dobro uređen skup tada njegov neprazni podskup $Y \cap X_{i_0}$ ima najmanji element: označimo ga s y_0. Tvrdimo da je y_0 najmanji element skupa Y, tj. da za sve $z \in Y \setminus \{y_0\}$ vrijedi $y_0 R_{i_0} z$. Neka je $z \in Y \setminus \{y_0\}$ proizvoljan. Pošto je $Y \subseteq \bigcup_{i\in I} X_i$ tada postoji $i \in I$ takav da je $z \in X_i$. Već smo bili naveli da je $\mathcal{U}$ linearno uređen skup, pa vrijedi barem jedno od:
$(X_i, R_i) \prec (X_{i_0}, R_{i_0})$ ili $(X_i, R_i) = (X_{i_0}, R_{i_0})$ ili $(X_{i_0}, R_{i_0}) \prec (X_i, R_i)$.

Pretpostavimo prvo da je $(X_i, R_i) \prec (X_{i_0}, R_{i_0})$. Ako bi vrijedilo $z R_{i_0} y_0$ tada iz $z, y_0 \in Y \cap X_{i_0}$ slijedi da je z manji od najmanjeg elementa iz $Y \cap X_{i_0}$, što je nemoguće. To znači da u ovom slučaju mora vrijediti $y_0 R_{i_0} z$. Ako je $(X_i, R_i) = (X_{i_0}, R_{i_0})$ tada iz $z \in Y \cap X_i$ i $X_i = X_{i_0}$, te činjenice da je y_0 najmanji element od $Y \cap X_{i_0}$, slijedi da je y_0 manji od z. Ako je $(X_{i_0}, R_{i_0}) \prec (X_i, R_i)$ tada je po definiciji R_{i_0} pravi podskup od R_i, te je X_{i_0} inicijalni segment od X_i.
Pretpostavimo da je $z \in X_i$ i $z R_i y_0$. Tada je $z \in X_{i_0}$ (jer je $y_0 \in X_{i_0}$ i X_{i_0} je inicijalni segment od X_i.) Time imamo da je $z \in Y \cap X_{i_0}$, te je z manji od y, što je nemoguće. Time smo dokazali da je $\mathcal{U}$ dobro uređen skup, tj. da je $\mathcal{U} \in \mathcal{D}$. Iz Zornove leme slijedi da za parcijalno uređen skup $(\mathcal{D}, \prec)$ postoji maksimalni element: označimo ga s (A_0, R_0).

Tvrdimo da je $A = A_0$. Pretpostavimo suprotno, tj. da postoji $a \in A \setminus A_0$. Definiramo binarnu relaciju R_1 na skupu $A_0 \bigcup \{a\}$ ovako:

$$R_1 = R_0 \bigcup \{(x, a) : x \in A_0\},$$

tj. relaciju R_0 dopunimo tako da definiramo da je element a veći od svih elemenata iz A_0.

Tvrdimo da je skup $A_0 \bigcup \{a\}$ dobro uređen relacijom R_1. U tu svrhu redom provjeravamo tražena svojstva relacije dobrog uređaja.

- *irefleksivnost*
  Ako je $x \in A_0$ tada iz činjenice da je (A_0, R_0) dobro uređen skup, tj. da je relacija R_0 irefleksivna, slijedi da ne vrijedi $x R_0 x$, a onda ni $x R_1 x$. Ne vrijedi ni $a R_1 a$, jer je po pretpostavci $a \in A \setminus A_0$.
- *tranzitivnost*
  Neka su $x, y, z \in A_0 \bigcup \{a\}$ takvi da je $x R_1 y$ i $y R_1 z$. Očito je $x \neq a$ i $y \neq a$. Promatramo dva slučaja:

  (i) $z \in A_0$; Tada vrijedi $x R_1 z$ jer je relacija R_0 tranzitivna;

(ii) $z = a$; Tada vrijedi xR_1z zbog $x \in A_0$ i definicije relacije R_1.

- *linearnost*
  Neka su $x, y \in A_0 \bigcup \{a\}$ i $x \neq y$. Ako vrijedi $x, y \in A_0$ tada su oni R_1–usporedivi, jer su R_0–usporedivi. Ako je $x = a$ ili $y = a$ tada R_1-usporedivost slijedi iz definicije relacije R_1.
- *dobra uređenost*
  Neka je X neprazni podskup od $A_0 \bigcup \{a\}$. Ako je $X \cap A_0 \neq \emptyset$ tada taj presjek ima najmanji element u odnosu na relaciju R_0 (po pretpostavci je ta relacija dobar uređaj). No, iz definicije relacije R_1 slijedi da je najmanji element u odnosu na relaciju R_0 ujedno najmanji element u odnosu na relaciju R_1. Ako pak je $X \cap A_0 = \emptyset$ tada je očito $X = \{a\}$, pa X ima najmanji element.

Iz toga slijedi da je $(A_0 \bigcup \{a\}, R_1) \in \mathcal{D}$. Pošto je očito $(A_0, R_0) \prec (A_0 \bigcup \{a\}, R_1)$, tada imamo da (A_0, R_0) nije maksimalni element od $\mathcal{D}$, što je kontradikcija.

Time smo dokazali da je (A, R_0) dobro uređen skup, a i da iz Zornove leme slijedi Zermelov teorem o dobrom uređaju. Za dokaz vidi i knjige [11], [19], [26] i [32].

7. Dokažite da aksiom izbora povlači Zornovu lemu.
   Dokaz. Neka je $(A, <)$ parcijalno uređen skup čiji svaki neprazni lanac ima gornju među. Neka je $\mathcal{L} = \{L : L \text{ je lanac od } A\}$. Uočimo da je $\mathcal{L} \neq \emptyset$, jer je primjerice $\emptyset \in \mathcal{L}$. Za svaki $L \in \mathcal{L}$ neka je $M(L) = \{a \in A : (\forall x \in L)(x \leq a)\}$, tj. $M(L)$ je skup svih gornjih međa skupa L. Iz početne pretpostavke imamo da je za svaki $L \in \mathcal{L}$ skup $M(L)$ neprazan. Dokaz ćemo provesti svođenjem na kontradikciju. Pretpostavimo da za skup A ne postoji maksimalni element. Primijetimo da je za sve $L \in \mathcal{L}$ skup $M(L) \setminus L$ neprazan. (Ako je $M(L) \setminus L = \emptyset$ tada je $M(L) \subseteq L$. Pošto je po pretpostavci $M(L)$ neprazan skup i L je lanac, tada skup L sadrži najveći element. Taj najveći element bi tada bio maksimalni element od A, što je suprotno prethodnoj pretpostavci.)

   Uočimo zatim da skup $(A, <)$ nije lanac, jer bi inače po pretpostavci imao gornju među, a ona bi bila maksimalni element od A. To znači da $A \notin \mathcal{L}$. Neka je $S = \{M(L) \setminus L : L \in \mathcal{L}\}$. Iz AC slijedi da postoji funkcija $g : \mathcal{P}(A) \setminus \{\emptyset\} \to A$, takva da za sve $B \in \mathcal{P}(A) \setminus \{\emptyset\}$ vrijedi $g(B) \in B$ (vidi zadatak 2).

   Bili smo prije primijetili da za sve lance L od A vrijedi $M(L) \setminus L \neq \emptyset$, pa je skup S podskup domene funkcije g. Sada definiramo funkciju

$$f : \mathcal{L} \to \mathcal{P}(A) \setminus \{\emptyset\}, \quad \text{sa} \quad f(L) = M(L) \setminus L,$$

   te konačno funkciju h kao kompoziciju $h = (g \mid_S) \circ f$. Primijetimo da za sve $L \in \mathcal{L}$ vrijedi

$$h(L) = g(f(L)) = g(M(L) \setminus L) \in M(L) \setminus L, \text{ tj.}$$

$$h(L) \in M(L) \setminus L \qquad (*)$$

Za $X \subseteq A$ kažemo da je inicijalni segment ako za svaki $y \in A$ i $x \in X$ iz činjenice $y < x$ slijedi $y \in X$. Lako je vidjeti da je svaki inicijalni segment od A ili početni komad od A ili pak je jednak A. Inicijalni segment od A koji je različit od A nazivamo pravi inicijalni segment.

Označimo s $\mathcal{L}_0$ podskup skupa $\mathcal{L}$ koji sadrži sve neprazne lance L od A takve da za sve inicijalne segmente $X \subset L$ (pravi podskup!) vrijedi:

$$h(X) = \inf{}_L(L \setminus X) \qquad (**)$$

Primijetimo prvo da je $\mathcal{L}_0 \neq \emptyset$, jer je $\{h(\emptyset)\}$ lanac (jednočlan skup!) koji pripada $\mathcal{L}_0$. (Pošto je $\emptyset$ lanac, tj. $\emptyset \in \mathcal{L}$, tada je funkcija h definirana na $\emptyset$. Jedini pravi inicijalni segment od $\{h(\emptyset)\}$ je $\emptyset$. To znači da uvjet $(**)$ treba provjeriti samo za $X = \emptyset$. No, očito vrijedi:

$$\inf{}_{\{h(\emptyset)\}}\Big(\{h(\emptyset)\} \setminus \emptyset\Big) = h(\emptyset).$$

Sada dokazujemo pomoćnu tvrdnju da za sve lance L_1 i L_2 iz $\mathcal{L}_0$ vrijedi: $L_1 \subseteq L_2$ ili $L_2 \subseteq L_1$. Pokažimo prvo da je $\{h(\emptyset)\}$ inicijalni segment koji pripada $L_1 \cap L_2$. Pošto je $\emptyset$ inicijalni segment od L_1 i L_2, te $L_1, L_2 \in \mathcal{L}_0$, tada iz definicije skupa $\mathcal{L}_0$, tj. $(**)$ slijedi:

$$\inf{}_{L_1}(L_1 \setminus \emptyset) = h(\emptyset) = \inf{}_{L_2}(L_2 \setminus \emptyset).$$

Iz toga slijedi $h(\emptyset) \in L_1 \cap L_2$, te da je to najmanji element od $L_1 \cap L_2$. No, iz toga direktno slijedi da je $\{h(\emptyset)\}$ zajednički inicijalni segment od L_1 i L_2.

Označimo sa $\mathcal{Z}$ uniju svih zajedničkih inicijalnih segmenata od L_1 i L_2. Iz prethodnih razmatranja slijedi $\mathcal{Z} \neq \emptyset$, jer je $h(\emptyset) \in \mathcal{Z}$. Primijetimo da je $\mathcal{Z}$ zajednički inicijalni segment od L_1 i L_2. (Neka je $x \in \mathcal{Z}$ i $y \in L_1$ takvi da je $y < x$. Iz definicije skupa $\mathcal{Z}$ slijedi da postoji zajednički inicijalni segment X od L_1 i L_2 tako da je $x \in X$. Tada je $y \in X$, a onda imamo i $y \in \mathcal{Z}$.) Uočimo da je funkcija h definirana na skupu $\mathcal{Z}$, jer je $\mathcal{Z} \subseteq L_1$ i L_1 je lanac (tada je i $\mathcal{Z}$ također lanac, tj. $\mathcal{Z} \in \mathcal{L}$). Iz svojstva funkcije h slijedi $h(\mathcal{Z}) \in M(\mathcal{Z}) \setminus \mathcal{Z}$, a onda posebno iz toga slijedi:

$$h(\mathcal{Z}) \notin \mathcal{Z} \qquad (***)$$

Pretpostavimo da je $\mathcal{Z}$ pravi podskup od L_1 i od L_2. Tada iz definicije skupa $\mathcal{L}_0$ slijedi:

$$h(\mathcal{Z}) = \inf{}_{L_1}(L_1 \setminus \mathcal{Z}) \in L_1.$$

Analogno, dobivamo da je $h(\mathcal{Z}) \in L_2$.

Tvrdimo da je $\mathcal{Z} \cup \{h(\mathcal{Z})\}$ zajednički inicijalni segment od L_1 i L_2. U svrhu tog dokaza izaberimo $x \in \mathcal{Z} \cup \{h(\mathcal{Z})\}$ i $y \in L_1$, takve da je $y < x$. Promatramo dva slučaja:

a) $x \in \mathcal{Z}$;
Bili smo dokazali da je $\mathcal{Z}$ inicijalni segment od L_1, pa je $y \in \mathcal{Z}$.

b) $x = h(\mathcal{Z})$;
Ako bi vrijedilo $y \in L_1 \setminus \mathcal{Z}$ tada iz $h(\mathcal{Z}) = \inf{}_{L_1}(L_1 \setminus \mathcal{Z})$ slijedi $h(\mathcal{Z}) < y$. No, to je kontradikcija s pretpostavkom da je $y < h(\mathcal{Z})$. To znači da i u ovom slučaju mora vrijediti $y \in \mathcal{Z}$.

Rezimirajmo što smo sve definirali i dokazali iz pretpostavke da je $\mathcal{Z}$ pravi podskup od L_1 i L_2 :

- $\mathcal{Z}$ je unija zajedničkih inicijalnih segmenata lanaca L_1 i L_2;
- $h(\mathcal{Z}) \notin \mathcal{Z}$ (vidi $(***)$);
- $\mathcal{Z} \cup h(\mathcal{Z})$ je zajednički inicijalni segment od L_1 i L_2.

Očito je da sve tri prethodno navedene činjenice ne mogu biti istinite, tj. pretpostavka da je $\mathcal{Z}$ pravi podskup od L_1 i L_2 vodi na kontradikciju. Time smo dokazali da je $\mathcal{Z} = L_1$ ili $\mathcal{Z} = L_2$.

Pošto je iz definicije skupa $\mathcal{Z}$ jasno da vrijedi $\mathcal{Z} \subseteq L_1 \cap L_2$, tada je $L_1 \subseteq L_2$ ili $L_2 \subseteq L_1$. Time smo dokazali da je skup $(\mathcal{L}_0, \subset)$ lanac. Označimo:

$$\mathcal{L}_0^* = \bigcup_{X \in \mathcal{L}_0} X.$$

Pošto je $(\mathcal{L}_0, \subset)$ lanac tada je i $\mathcal{L}_0^*$ lanac.

Tvrdimo da je $\mathcal{L}_0^* \cup \{h(\mathcal{L}_0^*)\} \in \mathcal{L}_0^*$. (Ako je X pravi inicijalni segment od $\mathcal{L}_0^*$ tada iz definicije skupa $\mathcal{L}_0^*$ slijedi da postoji lanac $Y \in \mathcal{L}_0$ takav da je $X \subseteq Y$. Sada iz definicije skupa $\mathcal{L}_0$ slijedi:

$$h(X) \overset{(**)}{=} \inf{}_Y(Y \setminus X).$$

Neka je $x_0 \in \mathcal{L}_0^*$ donja međa od $\mathcal{L}_0^* \setminus X$. Tada postoji $Y' \in \mathcal{L}_0$ takav da je $x_0 \in Y'$ i $X \subset Y'$. Po definiciji skupa $\mathcal{L}_0$ imamo $\inf{}_Y(Y \setminus X) = h(X) = \inf{}_{Y'}(Y' \setminus X)$,

što znači da je $x_0 \leq \inf_Y(Y \setminus X)$, iz čega slijedi $\inf_Y(Y \setminus X) = \inf_{\mathcal{L}_0^*}(\mathcal{L}_0^* \setminus X)$ Dakle, dobili smo:

$$h(X) = \inf_{\mathcal{L}_0^*}(\mathcal{L}_0^* \setminus X)\,.$$

Kako je X bio proizvoljan vidimo da vrijedi $\mathcal{L}_0^* \in \mathcal{L}_0$. Bili smo primijetili sa je $\mathcal{L}_0^*$ lanac, pa je funkcija h definirana na $\mathcal{L}_0^*$. Promotrimo lanac

$$\mathcal{C} = \mathcal{L}_0^* \cup \{h(\mathcal{L}_0^*)\}\,.$$

Neka je X pravi inicijalni segment od $\mathcal{C}$. Imamo dva slučaja:

1° X je pravi inicijalni segment od $\mathcal{L}_0^*$. Tada je $h(X) = \inf_{\mathcal{L}_0^*}(\mathcal{L}_0^* \setminus X)$. Kako je $h(\mathcal{L}_0^*)$ gornja međa od $\mathcal{L}_0^*$ vidimo da je $\inf_{\mathcal{L}_0^*}(\mathcal{L}_0^* \setminus X) = \inf_{\mathcal{C}}(\mathcal{C} \setminus X)$.

2° $X = \mathcal{L}_0^*$. Tada je $\mathcal{C} \setminus X = \mathcal{C} \setminus \mathcal{L}_0^* = \{h(\mathcal{L}_0^*)\}$, pa je $\inf_{\mathcal{C}}(\mathcal{C} \setminus X) = \inf_{\mathcal{C}}\{h(\mathcal{L}_0^*)\} = h(\mathcal{L}_0^*)$.

Dakle, dokazali smo da je $\mathcal{C} \in \mathcal{L}_0$. No tada je $\mathcal{C} \bigcup_{X \in \mathcal{L}_0} X = \mathcal{L}_0^*$, odakle imamo $h(\mathcal{L}_0^*) \in \mathcal{L}_0^*$, a kako je $\mathcal{L}_0^*$ lanac po $(*)$ mora biti $h(\mathcal{L}_0^*) \in M(\mathcal{L}_0^*) \setminus \mathcal{L}_0^*$ što je kontradikcija.

Time smo dobili da pretpostavka da skup $(A, <)$ nema niti jedan maksimalan element vodi na kontradikciju. Time je završen dokaz da aksiom izbora povlači Zornovu lemu. Za dokaz vidi i knjige [11], [18], [26] i [29].

8. Dokažite da Hartogsov teorem povlači aksiom izbora.
(Dokaz možete vidjeti primjerice u [8]).

9. Dokažite da teorem Tarskog povlači aksiom izbora.

10. Dokažite da Hausdorffov princip maksimalnosti povlači teorem Tarskog.

11. Dokažite korolar 2.56.
Dokaz. Primijetimo prvo da iz teorema 2.55. slijedi da postoji maksimum skupa $\{\lambda, \mu\}$. Radi određenosti neka je λ maksimum tog skupa. Očito je $\lambda \leq \lambda + \mu$. Kako bi dokazali obratnu nejednakost, prvo primijetimo:
$\lambda + \mu \leq \lambda \cdot \mu + \lambda \cdot \lambda \leq \lambda \cdot \lambda + \lambda \cdot \lambda = 2\lambda^2 = 2\lambda \leq \lambda \cdot \lambda = \lambda^2 = \lambda$

Iz Cantor, Schröder, Bernsteinovog teorema slijedi da je $\lambda + \mu = \lambda$.

Očito je $\lambda \cdot \mu \leq \lambda \cdot \lambda = \lambda^2 = \lambda$, te $\lambda \leq \lambda \cdot \mu$. Iz Cantor, Schröder, Bernsteinovog teorema slijedi $\lambda \cdot \mu = \lambda$.

12. Neka su α i β ordinalni brojevi takvi da je $\alpha \leq \beta$. Dokažite da je tada $\aleph_\alpha + \aleph_\beta = \aleph_\alpha \cdot \aleph_\beta = \aleph_\beta$.

13. Dokažite da opća hipoteza kontinuuma povlači aksiom izbora.
Uputa. Vidi [17], [18] i [20], te članak L. Gillman, *Two Classical Surprises Concerning the Axiom of Choice and the Continuum Hypothesis*, American Mathematical Monthly, 109, June–July 2002.

2.6 Zermelo–Fraenkelova teorija skupova

Kao što smo već bili naveli u uvodu, prvi prijedlog aksiomatizacije teorije skupova dao je Ernst Zermelo 1908. godine. Zermelo je bio dokazao da se svaki skup može dobro urediti. Nakon velikih kritika njegovog neočekivanog rezultata, Zermelo je pobrojao aksiome koje je koristio.

Ernst Zermelo, 1871.–1953.

A. Fraenkel je 1922. godine precizirao shemu aksioma separacije.

Abraham Fraenkel, 1891.–1965.

Zatim su A. Fraenkel i T. Skolem predložili shemu aksioma zamjene kao još jedan novi aksiom.

Thoralf Skolem, 1887.–1963.

J. von Neumann je eksplicirao aksiom dobre utemeljenosti i definirao ordinalne brojeve.

John von Neumann, 1903.–1957.

Sada rezimiramo definiciju teorije ZF. Zermelo–Fraenkelova teorija skupova, ili kratko ZF, je jedna teorija prvog reda. Formule teorije ZF gradimo pomoću varijabli, logičkih veznika i kvantifikatora, te dva dvomjesna relacijska simbola, koje označavamo sa $\in$ i $=$. Prisjetimo se aksioma teorije ZF:

aksiom ekstenzionalnosti

aksiom praznog skupa

aksiom para

aksiom unije

aksiom partitivnog skupa

aksiom izbora

aksiom dobre utemeljenosti

aksiom beskonačnosti

shema aksioma separacije

shema aksioma zamjene

Sistem aksioma teorije ZF nije nezavisan. Ne promatra se minimalan skup aksioma jer je na ovakav način omogućeno razmatranje više zanimljivih podteorija od ZF.

Na samom početku bili smo naveli da je osnovno pitanje kolegija: "Što je skup?" Sada je vrijeme da pokušamo rezimirati kako smo pokušali odgovoriti na spomenuto pitanje. Skupovi su objekti koji pripadaju strukturi koju nazivamo kumulativna hijerhija (nisu svi objekti u kumulativnoj hijerahiji skupovi – neki objekti su prave klase). Kako bi iz kumulativne hijerahije izdvojili objekte koji su skupovi napisali smo listu aksioma, koje kratko nazivamo Zermelo–Fraenkelova teorija skupova. Koliko smo time zapravo uspjeli opisati skupove, teško je pitanje. Svakako neodlučivost nekih problema kao što je hipoteza kontinuuma nije dobar signal da smo sasvim uspjeli. Već dugo vremena među matematičarima koji se bave teorijom skupova traju rasprave o tome koje nove akisome bi trebalo dodati teoriji ZF. Ovdje ćemo navesi primjer prijedloga jednog takvog aksioma. To je Martinov aksiom o determiniranosti igara. U tu svrhu prvo definiramo neke pojmove. Neka je X neki skup nizova nula i jedinica. Dva igrača, koje označavamo sa I i II, igraju igru tako da naizmjence biraju 0 ili 1. Igrač I pobjeđuje ako niz pripada X, a inače pobjeđuje II. Kažemo da neki igrač ima pobjedničku strategiju ako za svaki potez protivnika ima odgovor što treba izabrati kako bi na kraju pobijedio.

Martinov aksiom o determiniranosti igara:

Za svaki skup X nizova nula i jedinica barem jedan igrač ima pobjedničku strategiju.

Za skup X nizova nula i jedinica sa AD(X) označavamo pripadni Martinov aksiom.

Napomena 2.59. *Primjenom AC slijedi da postoji skup X tako da je AD(X) lažno. U drugu ruku, ZF+AD(X) povlači da je Banach–Tarskijeva dekompozicija nemoguća.*

O Martinovom aksiomu možete više čitati u [3].

Na samom kraju navodimo neke teme iz teorije skupova koje bi bile prirodni nastavak sadržaja kojeg smo mi proučavali.

1. nezavisnost aksioma izbora – konstruktibilna hijerahija
2. nezavisnost hipoteze kontinuuma – metoda forcinga
3. novi aksiomi teorije skupova – primjerice Martinov aksiom o determiniranosti igara
4. kardinalna aritmetika; nedostiživi kardinalni brojevi

5. deskriptivna teorija skupova

Za druge teme vidite primjerice [13].

Zadaci

1. Dokažite da iz sheme aksioma zamjene slijedi shema aksioma separacije.

2. Dokažite da iz sheme aksioma separacije slijedi aksiom praznog skupa.

3. Dokažite da iz sheme aksioma zamjene i aksioma partitivnog skupa slijedi aksiom para.
   Dokaz. Neka je $F(x, y) \equiv (x = \emptyset \wedge y = a) \vee (x = \{\emptyset\} \wedge y = b)$. Iz aksioma partitivnog skupa slijedi da postoji skup $\mathcal{P}^2(\emptyset) = \{\emptyset, \{\emptyset\}\}$. Sada primjenom sheme aksioma zamjene na F te na skup $\mathcal{P}^2(\emptyset)$ slijedi egzistencija para $\{a, b\}$.

Dodatak: Goodsteinov teorem

U ovom dodatku razmatrat ćemo jedan teorem. Tri su razloga zašto promatramo taj teorem. Prvi je razlog to što je tvrdnja teorema pomalo čudna na prvi pogled, čak izgleda nevjerojatna. Ovaj razlog je najmanje važan, ali većina ljudi upravo to vide kao najzanimljiviji aspekt Goodsteinovog teorema. Drugi razlog je da se za njegov dokaz koriste beskonačni ordinalni brojevi, iako teorem govori o prirodnim brojevima. Treći razlog je zapravo najvažniji, ali je najvjerojatnije najmanje razumljiv. Gödelov prvi teorem nepotpunosti govori da svaku istinitu tvrdnju o prirodnim brojevima nije moguće dokazati pomoću Peanovih aksioma. Dokazano je da Goodsteinov teorem nije moguće dokazati samo pomoću Peanovih aksioma, tj. da je za njegov dokaz nužno koristiti beskonačne ordinalne brojeve.

Kako bi mogli izreći Goodsteinov teorem moramo definirati prikaz prirodnog broja u superbazi i Goodsteinov niz prirodnog broja. Te pojmove nećemo strogo definirati već ćemo ih objasniti pomoću primjera.

Svima je poznat pojam prikaza broja u nekoj bazi. Npr. prikažimo brojeve 27 i 521 u bazi 2:

$$27 = 2^4 + 2^3 + 2^1 + 2^0 \qquad \text{i} \qquad 521 = 2^9 + 2^3 + 2^0$$

Prikazati neki broj u superbazi b znači prvo broj prikazati u bazi b, zatim eksponente prikazati u bazi b, pa eksponente eksponenata prikazati u bazi b, itd. Pogledajmo to na primjeru prikaza brojeva 27 i 521 u superbazi 2:

$$27 = 2^4 + 2^3 + 2^1 + 2^0 = 2^{2^2} + 2^{2+1} + 2^1 + 2^0$$

$$521 = 2^9 + 2^3 + 2^0 = 2^{2^3+1} + 2^{2+1} + 2^0 = 2^{2^{2+1}+1} + 2^{2+1} + 2^0$$

Ovdje je kao primjer dan i prikaz broja 521 u superbazi 3:

$$521 = 2 \cdot 3^5 + 3^3 + 2 \cdot 3 + 2 = 2 \cdot 3^{3+2} + 3^3 + 2 \cdot 3 + 2$$

Pojam Goodsteinovog niza definiramo prvo na primjeru broja 8. Prvi član Goodsteinovog niza broja 8 je on sam. Označavamo ga sa $(8)_1 = 8$. Kako bi dobili drugi član niza prikažimo prvo broj 8 u superbazi 2, tj. $8 = 2^{2+1}$. Umjesto svih dvojki u prikazu 2^{2+1} napišemo trojke, pa dobivamo 3^{3+1}. Zatim od tako dobivenog broja

oduzmemo 1. Time smo dobili drugi član Goodsteinovog niza, tj. $(8)_2 = 80$. Prikažimo sada broj 80 u superbazi 3, zatim zamijenimo sve trojke s četvorkama, te oduzmemo jedan. Dobili smo $(8)_3 = 553$. Nadamo se da je jasan daljnji postupak konstrukcije Goodsteinovog niza. Bez daljnjih detaljnih objašnjena navodimo nekoliko prvih članova Goodsteinovog niza broja 8.

$$
\begin{array}{lll}
 & (8)_1 = & 8 \\
 & & \\
\textit{superbaza } 2 & & 8 = 2^{2+1} \\
2 \mapsto 3 & & 3^{3+1} = 81 \\
-1 & (8)_2 = & 80 \\
 & & \\
\textit{superbaza } 3 & & 80 = 2 \cdot 3^3 + 2 \cdot 3^2 + 2 \cdot 3 + 2 \\
3 \mapsto 4 & & 2 \cdot 4^4 + 2 \cdot 4^2 + 2 \cdot 4 + 2 = 554 \\
-1 & (8)_3 = & 553 \\
 & & \\
\textit{superbaza } 4 & & 553 = 2 \cdot 4^4 + 2 \cdot 4^2 + 2 \cdot 4 + 1 \\
4 \mapsto 5 & & 2 \cdot 5^5 + 2 \cdot 5^2 + 2 \cdot 5 + 1 = 6\ 311 \\
-1 & (8)_4 = & 6\ 310 \\
 & & \\
\textit{superbaza } 5 & & 6\ 310 = 2 \cdot 5^5 + 2 \cdot 5^2 + 2 \cdot 5 \\
5 \mapsto 6 & & 2 \cdot 6^6 + 2 \cdot 6^2 + 2 \cdot 6 = 93\ 396 \\
-1 & (8)_5 = & 93\ 395 \\
 & & \\
\textit{superbaza } 6 & & 93\ 395 = 2 \cdot 6^6 + 2 \cdot 6^2 + 6 + 5 \\
 & \vdots & \\
 & (8)_6 = & 1\ 647\ 195 \\
 & (8)_7 = & 33\ 554\ 571 \\
 & (8)_8 = & 774\ 841\ 151 \\
 & (8)_9 = & 20\ 000\ 000\ 211 \\
 & (8)_{10} = & 570\ 623\ 341\ 475 \\
 & \vdots &
\end{array}
$$

Sada navodimo nekoliko prvih članova Goodsteinovog niza broja 25.

$$\begin{aligned}
(25)_1 = 25 &= 2^{2^2} + 2^{2+1} + 1 \\
&\quad 3^{3^3} + 3^{3+1} + 1 \\
(25)_2 &= 3^{3^3} + 3^{3+1} \approx 10^{13} \\
&\quad 4^{4^4} + 4^{4+1} \\
(25)_3 &= 4^{4^4} + 3 \cdot 4^4 + 3 \cdot 4^3 + 3 \cdot 4^2 + 3 \cdot 4 + 3 \approx 10^{81} \\
&\quad 5^{5^5} + 3 \cdot 5^5 + 3 \cdot 5^3 + 3 \cdot 5^2 + 3 \cdot 5 + 3 \\
(25)_4 &= 5^{5^5} + 3 \cdot 5^5 + 3 \cdot 5^3 + 3 \cdot 5^2 + 3 \cdot 5 + 2 \approx 10^{2\,216}
\end{aligned}$$

Evo još desetak prvih članova Goodsteinovog niza broja 266.

$$\begin{aligned}
(266)_1 = 266 = 2^{2^{2+1}} + 2^{2+1} + 2 &\geq 2^{2^3} \simeq 3 \times 10^2 \\
(266)_2 = 3^{3^{3+1}} + 3^{3+1} + 2 &\geq 3^{3^4} \simeq 4 \times 10^{38} \\
(266)_3 = 4^{4^{4+1}} + 4^{4+1} + 1 &\geq 4^{4^5} \simeq 3 \times 10^{616} \\
(266)_4 = 5^{5^{5+1}} + 5^{5+1} &\geq 5^{5^6} \simeq 3 \times 10^{10921} \\
(266)_5 = 6^{6^{6+1}} + 5 \cdot 6^6 + 5 \cdot 6^5 + \ldots 5 \cdot 6 + 5 &\simeq 4 \times 10^{217832} \\
(266)_6 = 7^{7^{7+1}} + 5 \cdot 7^7 + 5 \cdot 7^5 + \ldots 5 \cdot 7 + 4 &\simeq 10^{4871822} \\
(266)_7 = 8^{8^{8+1}} + 5 \cdot 8^8 + 5 \cdot 8^5 + \ldots 5 \cdot 8 + 3 &\simeq 2 \times 10^{121210686} \\
(266)_8 = 9^{9^{9+1}} + 5 \cdot 9^9 + 5 \cdot 9^5 + \ldots 5 \cdot 9 + 2 &\simeq 5 \times 10^{3327237896} \\
(266)_9 = 10^{10^{10+1}} + 5 \cdot 10^{10} + 5 \cdot 10^5 + \ldots 5 \cdot 10 + 1 &\simeq 10^{10^{11}}
\end{aligned}$$

$$\vdots$$

Najvjerojatnije ste zaključili da Goodsteinovi nizovi brojeva 8, 25 i 266 teže prema beskonačnosti. No, prevarili ste se. R. L. Goodstein je dokazao 1944. godine sljedeći teorem.

Teorem. *Svaki Goodsteinov niz završava s nulom.*

Kako je to moguće? U prvi tren se čini nevjerojatno. Pokušat ćemo vas u istinitost Goodsteinovog teorema uvjeriti navodeći Goodsteinov niz broja 3.

superbaza 2	$(3)_1 = 3$	$= 2 + 1$
$2 \mapsto 3$		$3 + 1 = 4$
	4	
-1	$(3)_2 = 3$	
superbaza 3	3	
$3 \mapsto 4$	4	
-1	$(3)_3 = 3$	
superbaza 4	3	
$4 \mapsto 5$	3	
-1	$(3)_4 = 2$	
superbaza 5	2	
$5 \mapsto 6$	2	
-1	$(3)_5 = 1$	
superbaza 6	1	
$6 \mapsto 7$	1	
-1	$(3)_6 = 0$	

Uočite da je u jednom trenutku član Goodsteinovog niza manji od superbaze (u ovom slučaju to je $(3)_3$). Nakon toga članovi Goodsteinovog niza strogo padaju, pa pošto se radi o prirodnim brojevima niz mora završiti s nulom. Za neke prirodne brojeve član Goodsteinovog niza koji je manji od trenutne superbaze može biti vrlo velik. (Npr. duljina Goodsteinovog niza za broj 4 je broj koji ima više od 121 210 700 znamenaka).

Za strogi dokaz Goodsteinovog teorema koristi se transfinitna indukcija do ordinalnog broja ϵ_0. Ideja dokaza je vrlo jednostavna. Svakom članu Goodsteinovog niza se pridružuje beskonačni ordinalni broj manji od ϵ_0. Tada se dokaže da pridruženi ordinalni brojevi strogo padaju. Primjenom transfinitne indukcije do ordinalnog broja ϵ_0 tada slijedi da svaki strogo padajući niz ordinalnih brojeva mora završiti s nulom. Promotrimo pridruživanje ordinalnih brojeva članovima Goodsteinovog niza broja 4 (umjesto superbaze uvrštavamo ordinali broj ω).

$$
\begin{array}{ll}
4 = & 2^2 \\
 & \omega^\omega \\
 & \\
2 \mapsto 3 & 3^3 \\
-1 & 2 \cdot 3^2 + 2 \cdot 3 + 2 \\
 & \omega^2 \cdot 2 + \omega \cdot 2 + 2 \\
 & \\
(1{+}3 \text{ koraka}) & 2 \cdot 6^2 + 6 + 5 \\
 & \omega^2 \cdot 2 + \omega + 5 \\
 & \\
(1+3+6) & 2 \cdot 12^2 + 11 \\
 & \omega^2 \cdot 2 + 11 \\
 & \\
(1+3+6+12) & 24^2 + 23 \cdot 24 + 23 \\
 & \omega^2 + \omega \cdot 23 + 23 \\
 & \\
(1+3+6+12+24) & 48^2 + 22 \cdot 48 + 47 \\
 & \omega^2 + \omega \cdot 22 + 47 \\
 & \\
 & \vdots
\end{array}
$$

Pošto Goodsteinov teorem govori o prirodnim brojevima, prirodno se nameće pitanje može li se provesti dokaz tog teorema u kojem se neće koristiti beskonačni ordinalni brojevi. Godine 1982. je dokazano da se Goodsteinov teorem ne može dokazati primjenom samo prirodnih brojeva (točnije pomoću Peanovih aksioma). To znači da je za dokaz tog teorema nužna primjena beskonačnih ordinalnih brojeva. To je zapravo najvažnije u vezi Goodsteinovog teorema. Time je taj teorem u direktnoj vezi s Gödelovim teoremima nepotpunosti.

Sada dajemo dokaz Goodsteinovog teorema. Prvo definiramo funkcije koje prirodnom broju zapisanom u superbazi n pridružuju broj koji nastaje zamjenom superbaze n sa $n+1$.

Definicija 2.60. *Za svaki $n \in \mathbb{N}$, $n \geq 2$, definiramo funkciju $S_n : \mathbb{N} \to \mathbb{N}$ sa:*

$$S_n(0) = 0$$

$$S_n(k \cdot n^t) = k \cdot (n+1)^{S_n(t)}, \quad \textit{ako je} \quad k < n;$$

$$S_n(\sum_{i=0}^{d} k_i \cdot n^i) = \sum_{i=0}^{d} S_n(k_i \cdot n^i), \quad \textit{gdje je} \quad k_0, \ldots, k_d < n.$$

Definicija 2.61. *Induktivno definiramo niz funkcija* (g_n), *gdje je* $g_n : \mathbb{N} \to \mathbb{N}$, *ovako:*

$$g_2(m) = S_2(m) - 1$$

$$g_{n+1}(m) = S_{n+1}(g_n(m)) - 1$$

Uočite da je za sve $m \in \mathbb{N}$ upravo $(g_n(m))$ Goodsteinov niz broja m.

Teorem 2.62. *(R. L. Goodstein, 1944.)*
Za svaki $m \in \mathbb{N}$ *postoji* $n \in \mathbb{N}$ *tako da je* $g_n(m) = 0$.

Ponavljamo da je ideja dokaza Goodteinovog teorema vrlo jednostavna: članove Goodsteinovog niza ćemo kodirati ordinalnim brojevima manjim od ϵ_0, te dokazati da ti ordinalni brojevi strogo padaju. To znači da Goodsteinov niz mora biti konačan. U svrhu dokaza definiramo i sljedeći niz funkcija.

Definicija 2.63. *Neka je za sve* $n \in \mathbb{N}$, $n \geq 2$, *s* $f_n : \mathbb{N} \to \epsilon_0$ *označena funkcija koja je definirana sa:*

$$f_n(0) = 0$$

$$f_n(k \cdot n^t) = \omega^{f_n(t)} \cdot k, \quad \textit{pri čemu je} \quad k < n$$

$$f_n(\sum_{i=0}^{d} k_i \cdot n^i) = \sum_{i=0}^{d} f_n(k_i \cdot n^i), \quad \textit{gdje je} \quad k_0, \ldots, k_d < n$$

Objasnimo ukratko definiciju niza funkcija (f_n). Ako je neki broj m zapisan u superbazi n tada je $f_n(m)$ ordinalni broj koji je dobiven zamjenom svih n-ova u prikazu broja m s ω. Primjerice, vrijedi sljedeće:

$$f_5(3 \cdot 5^{5^4} + 2 \cdot 5^{5^2} + 4 \cdot 5^5 + 3 \cdot 5 + 2) = \omega^{\omega^4} \cdot 3 + \omega^{\omega^2} \cdot 2 + \omega^\omega \cdot 4 + \omega \cdot 3 + 2$$

Lema 2.64. *Za sve* $n, m \in \mathbb{N}$, $n \geq 2$, *vrijedi*

$$f_n(m) = f_{n+1}(S_n(m)).$$

Dokaz. Dokaz provodimo indukcijom po m. Za $m = 0$ imamo

$$f_{n+1}(S_n(0)) = f_{n+1}(0) = 0 = f_n(0).$$

Neka je $m \in \mathbb{N}$ takav da tvrdnja leme vrijedi za sve prirodne brojeve strogo manje od m. Neka je $n \in \mathbb{N}$ proizvoljan ($n \geq 2$). Napišimo broj m u bazi n (ovdje ne promatramo zapis u superbazi!), tj. neka je

$$m = \sum_{i=0}^{d} k_i \cdot n^i, \quad \text{gdje je} \quad k_0, \ldots, k_d < n.$$

Tada imamo:

$$\begin{aligned}
f_{n+1}(S_n(m)) &= f_{n+1}(S_n(\sum_{i=0}^{d} k_i \cdot n^i)) && = \text{(def. funkcije } S_n\text{)} \\
&= f_{n+1}(\sum_{i=0}^{d} S_n(k_i \cdot n^i)) && = \text{(def. funkcije } S_n\text{)} \\
&= f_{n+1}(\sum_{i=0}^{d} k_i \cdot (n+1)^{S_n(i)}) && = \text{(def. funkcije } f_{n+1}\text{)} \\
&= \sum_{i=0}^{d} f_{n+1}(k_i \cdot (n+1)^{S_n(i)}) && = \text{(def. funkcije } f_{n+1}\text{)} \\
&= \sum_{i=0}^{d} \omega^{f_{n+1}(S_n(i))} \cdot k_i && = \text{(pret. indukcije)} \\
&= \sum_{i=0}^{d} \omega^{f_n(i)} \cdot k_i && = \text{(def. funkcije } f_n\text{)} \\
&= \sum_{i=0}^{d} f_n(k_i \cdot n^i) && = \text{(def. funkcije } f_n\text{)} \\
&= f_n(\sum_{i=0}^{d} k_i \cdot n^i) && = f_n(m)
\end{aligned}$$

Q.E.D.

Lema 2.65. *Za sve $n, m \in \mathbb{N}$, $n \geq 2$ vrijedi $f_n(m+1) > f_n(m)$.*

Dokaz. Dokaz provodimo indukcijom po m. Za $m = 0$ imamo $f_n(1) = f_n(1 \cdot n^0) = \omega^{f_n(0)} = \omega^0 = 1$, a po definiciji je $f_n(0) = 0$. Time imamo da je $f_n(1) > f_n(0)$. Pretpostavimo da je $m \in \mathbb{N}$ takav da za sve prirodne brojeve koji su strogo manji od m tvrdnja vrijedi. Napišimo broj m u bazi n, tj. neka je

$$m = k_d \cdot n^d + k_{d-1} \cdot n^{d-1} + \ldots + k_1 \cdot n + k_0,$$

gdje je za sve $i \leq d$ ispunjeno $0 \leq k_i < n$. Promatramo dva slučaja:

a) $k_0 < n - 1$;

b) postoji s takav da je $k_s < n-1$, te je $k_{s-1} = k_{s-2} = \ldots = k_1 = k_0 = n-1$.

Promotrimo prvo slučaj a). Tada imamo

$$\begin{aligned} f_n(m+1) &= f_n(k_d \cdot n^d + k_{d-1} \cdot n^{d-1} + \ldots + k_1 \cdot n + k_0 + 1) \\ &= \omega^d \cdot k_d + \omega^{d-1} \cdot k_{d-1} + \ldots + \omega \cdot k_1 + k_0 + 1 \\ &> \omega^d \cdot k_d + \omega^{d-1} \cdot k_{d-1} + \ldots + \omega \cdot k_1 + k_0 \\ &= f_n(m). \end{aligned}$$

Promotrimo sada slučaj b). Iz uvjeta slijedi:

$$m = k_d \cdot n^d + \ldots + k_s \cdot n^s + (n-1) \cdot n^{s-1} + \ldots + (n-1) \cdot n + (n-1)$$

$$m + 1 = k_d \cdot n^d + \ldots + (k_s + 1) n^s$$

Tada imamo:

$$\begin{aligned} f_n(m) &= \omega^d \cdot k_d + \ldots + \omega^s \cdot k_s + \omega^{s-1} \cdot (n-1) + \ldots + \omega \cdot (n-1) + (n-1) \\ &\leq \omega^d \cdot k_d + \ldots + \omega^s \cdot k_s + \underbrace{\omega^{s-1} \cdot (n-1) + \ldots + \omega^{s-1} \cdot (n-1)}_{s} \\ &= \omega^d \cdot k_d + \ldots + \omega^s \cdot k_s + \omega^{s-1} \cdot (n-1) \cdot s \\ &< \omega^d \cdot k_d + \ldots + \omega^s \cdot k_s + \omega^s \\ &= \omega^d \cdot k_d + \omega^s \cdot (k_s + 1) \\ &= f_n(m+1). \end{aligned}$$

Q.E.D.

Lema 2.66. *Za sve $n, m \in \mathbb{N}$, $n \geq 2$, takve da je $g_n(m) > 0$ vrijedi*

$$f_{n+2}(g_{n+1}(m)) > f_{n+1}(g_n(m)).$$

Dokaz. Redom imamo:

$$\begin{aligned} f_{n+2}(g_{n+1}(m) &= f_{n+2}(S_{n+1}(g_n(m)) - 1) && < \text{ (lema 2.65.)} \\ &< f_{n+2}(S_{n+1}(g_n(m))) && = \text{ (lema 2.64.)} \\ &= f_{n+1}(g_n(m)) && \text{Q.E.D.} \end{aligned}$$

Dokaz Goodsteinovog teorema:
Pretpostavimo da je $m \in \mathbb{N}$ takav da su svi članovi niza $(g_n(m))$ strogo veći od nule. Tada iz leme 2.66. slijedi da imamo strogo padajući niz ordinalnih brojeva:

$$f_3(g_2(m)) \ > \ f_4(g_3(m)) \ < \ f_5(g_4(m)) \ < \ \ldots,$$

što je nemoguće. Q.E.D.

Više detalja o Goodsteinovom teoremu možete pročitati u [14], [19] i [31], odnosno u člancima L. D. Beklemishev, Worm Principle, preprint 219, Utrecht, 2003.; R. L. Goodstein, On the restricted ordinal theorem, Journal of Symbolic Logic, 9 (1944), 33–41; M. Vuković, Matematička indukcija i Goodsteinov teorem, Poučak – Časopis za metodiku i nastavu matematike, 13 (2003), 5–13; M. Vuković, Gödelovi teoremi nepotpunosti, MFL, 2002.

Bibliografija

[1] P. Aczel, *Non–well–founded sets*, CSLI Standford, 1988.

[2] M. Aiguer, G. Ziegler, *Proofs from the Book*, Springer, 1999.

[3] K. J. Barwise (ed.), *Handbook of mathematical logic, IV,* North–Holland Publising Company, Amsterdam, 1977.

[4] F. M. Brückler, V. Čačić, M. Doko, M. Vuković, *Zbirka zadataka iz teorije skupova*, web–izdanje, PMF–MO, Zagreb, 2008.
http://web.math.hr/∼vukovic/dodiplomska_nastava.htm

[5] V.Čačić, *Banach–Tarskijev paradoks*, diplomski rad, PMF–MO, Zagreb, 2002.

[6] V.Čačić, *Nezavisnost i relativna konzistentnost aksioma izbora i hipoteze kontinuuma*, magistarski rad, PMF–MO, Zagreb, 2007.

[7] P. J. Cohen, *Set Theory and the Continuum Hypothesis*, Dover Publications, 2008.

[8] K. J. Devlin, *Fundamentals of Contemporary Set Theory*, Springer, 1980.

[9] M. Doko, *Kardinalna aritmetika*, diplomski rad, PMF–MO, Zagreb, 2006.

[10] F. R. Drake, *Set Theory: An Introduction to Large Cardinals*, North–Holland Publishing Company, 1974.

[11] F. R. Drake, D. Singh, *Intermediate Set Theory*, John Wiley & Sons, 1996.

[12] H. Enderton, *Elements of Set Theory*, Academic Press, 1977.

[13] M. Foreman, A. Kanamori, M. Magidor (eds.), *Handbook of Set Theory*, Springer, 2010. `http://www.tau.ac.il/∼rinot/host.html`

[14] J. M. Henle, *An outline of set theory*, Springer, 1986.

[15] M. Holz, K. Steffens, E. Weitz, *Introduction to Cardinal Arithmetic*, Birkhäuser, 1999.

[16] K. Hrbacek, T. Jech, *Introduction to Set Theory*, Third Edition, Marcel Dekker, Inc., New York, 1999.

[17] T. Jech, *The Axiom of Choice*, Dover Publications, 1973.

[18] T. Jech, *Set Theory*, The Third Millenium Edition, Springer, 2000.

[19] W. Just, M. Weese, *Discovering Modern Set Theory 1,2*, AMS, 1996.

[20] P. Komjáth, V. Totik, *Problems and Theorems in Classical Set Theory*, Springer, 2000.

[21] K. Kunen, *Set Theory—An Introduction to Independence Proofs*, North-Holland Publishing Company, 1992.

[22] Dj. Kurepa, *Teorija skupova*, Tehnička knjiga, Zagreb, 1951.

[23] S. Kurepa, *Uvod u matematiku*, Tehnička knjiga, Zagreb, 1970.

[24] I. A. Lavrov, L. L. Maksimova, *Zbornik zadač po teorii množestv. mat. logik i teorii algoritmov* (rus.), Nauka, Moskva, 1986.

[25] I. A. Lavrov, L. L. Maksimova, *Problems in Set Theory, Mathematical Logic and the Theory of Algorithms*, Kluwer Academic/Plenum Publisher, 2003.

[26] S. Lipschutz, *Set Theory and Related Topics*, Schaumm's outline series, Second Edition, McGraw–Hill, 1998.

[27] Y. Moschovakis, *Notes on Set Theory*, Springer, 2006.

[28] D. Monk, *Introduction to Set Theory*, McGraw–Hill, Inc., New York, 1969.

[29] P. Papić, *Uvod u teoriju skupova*, HMD, Zagreb, 2000.

[30] B. Poizat, *A Course in Model Theory*, Springer, 2000.

[31] M. D. Potter, *Mengentheorie*, Spektrum Akademischer Verlag, 1990.

[32] H. Rubin, J. Rubin, *Equivalents of the Axiom of Choice*, North–Holland, 1970.

[33] L. E. Siegler, *Exercises in Set Theory*, Springer, New York, 1976.

[34] S. Shelah, *Cardinal Arithmetic*, Clarendon Press, Oxford, 1994.

[35] A. Shen, N. K. Vereshchagin, *Basic Set Theory*, AMS, 2002.

[36] Z. Šikić, *Kako je stvarana novovjekovna matematika*, Školska knjiga, Zagreb, 1989.

[37] N. J. Vilenkin, *Priče o skupovima*, Školska knjiga, Zagreb, 1975.

[38] M. Vuković, *Matematička logika*, Element, Zagreb, 2009.

[39] M. Vuković, *O aksiomu izbora, čarapama i cipelama*, Poučak, 39 (2009), 54–60

[40] S. Wagon, *Banach–Tarski Paradox*, Cambridge University Press, 1999.

Indeks